VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

METODIKA HODNOCENÍ INFORMAČNÍCH SYSTÉMŮ
INFORMATION SYSTEMS ASSESSMENT METHODOLOGY

DIZERTAČNÍ PRÁCE
DOCTORAL THESIS

AUTOR PRÁCE — **Ing. Lukáš Novák**
AUTHOR

ŠKOLITEL — **doc. Ing. Miloš Koch, CSc.**
SUPERVISOR

BRNO 2017

Vysoké učení technické v Brně, Fakulta podnikatelská

Akademický rok: 2017/18

ZADÁNÍ DIZERTAČNÍ PRÁCE

student(ka): Ing. Lukáš Novák

který/která studuje v **doktorském studijním programu**

obor: **Řízení a ekonomika podniku (6208V097)**

Téma dizertační práce:

Metodika hodnocení informačních systémů

v anglickém jazyce:

Information Systems Assessment Methodology

Stručná charakteristika problematiky úkolu:

1. Úvod a cíl práce
2. Použité metody
3. Současný stav vědeckého poznání
4. Metodika hodnocení informačních systémů
5. Přínosy dizertační práce
6. Závěr

Cíle dizertační práce:

Cílem dizertační práce je navržení vlastní metodiky pro hodnocení informačních systémů. Předpokladem nové metodiky je navázat na předchozí výzkum a inovovat současné postupy a metodiky. Mezi dílčí kroky, které je třeba učinit k dosažení cíle, se řadí určení technik a identifikování hlavních kritérií, která by měla být brána v úvahu při hodnocení informačních systémů. Dále je nutné provést rešerši informačních zdrojů, analyzovat současný stav problematiky, realizovat primární výzkum pomocí hloubkových rozhovorů, vyhodnotit získaná data, vytvořit metodiku hodnocení informačních systémů a verifikovat ji kvalitativním přístupem pomocí případových studií.

Seznam odborné literatury:

BODDY, David, Albert BOONSTRA a Graham KENNEDY, 2008. Managing information systems: strategy and organisation. 3rd ed. New York: Prentice Hall/Financial Times. ISBN 978-0273716815.
DELONE William a Ephraim McLEAN, 2003. The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. J. Manage. Inf. Syst. 19, 4 (April 2003), 9-30.
CHA-JAN CHANG, Jerry a William R. KING, 2003. Measuring the Performance of Information Systems: A Functional Scorecard. J. Manage. Inf. Syst. 22(1), 85-115. DOI: 10.1080/07421222.2003.11045833.
IRANI, Zahir a Peter LOVE, 2008. Evaluating Information Systems: Public and private sector, Oxford: Elsevier. DOI: 10.1016/B978-0-7506-8587-0.50004-4
LAGSTEN, Jenny, 2011. Evaluating Information Systems according to Stakeholders: A Pragmatic Perspective and Method. Electronic Journal of Information Systems Evaluation. 14(1), 73-88. ISSN 15666379.
LOW, Chinyao a Ya CHEN, 2012. Criteria for the Evaluation of a Cloud-Based Hospital Information System Outsourcing Provider. Journal of Medical Systems. 36(6), 3543-3553. DOI: 10.1007/s10916-012-9829-z. ISSN 01485598.
SOLIC, Kresimir, Hrvoje OCEVCIC a Marin GOLUB, 2015. The information systems' security level assessment model based on an ontology and evidential reasoning approach. Computers. 55, 100-112. DOI: 10.1016/j.cose.2015.08.004. ISSN 01674048.
SVATÁ, Vlasta, 2011. Audit informačního systému. Praha: Professional Publishing. ISBN 978-80-7431-034-8.

Vedoucí dizertační práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání dizertační práce je stanoven časovým plánem akademického roku 2017/18.

V Brně, dne 15. 9. 2017

L.S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

Předseda oborové rady

Děkan

ANOTACE

Dizertační práce je orientovaná na oblast hodnocení informačních systémů a vymezuje hlavní nedostatky v provozu a řízení informačních systémů v návaznosti na procesy v oddělení informatiky, s částečným přesahem do ostatních částí podniku. Práce dále rozšiřuje současný pohled na hodnocení informačních systémů v podniku a v souladu s cílem práce definuje vlastní metodiku, která vymezuje konkrétní proces hodnocení a člení jeho obsah na jednotlivé dílčí celky. Navržená metodika umožňuje získat přehled o nedostatcích a možných opatřeních v oblasti provozu a řízení informačních systémů. Součástí práce je také kvalitativní ověření metodiky v malé, střední a velké společnosti pomocí případových studií.

KLÍČOVÁ SLOVA

Informační systémy, Hodnocení informačních systémů, Nedostatky v oblasti provozu a řízení informačních systémů, Bezpečnost informačních systémů, Audit informačních systémů, Řízení IT oddělení, Případová studie

ANNOTATION

The doctoral dissertation thesis is focused on assessment of information systems and defines the main deficiencies in operation and management of information systems in relation to processes in the department of informatics with partial overlapping into the other parts of the company. The thesis further extends the current view of assessment of information systems in the company and, in accordance with the goal of the work, it defines its own methodology, which defines the specific assessment process and subdivides its contents into individual units. The proposed methodology provides an overview of the deficiencies and possible measures in operation and management of information systems. Qualitative verification of methodology in small, medium and large companies using case studies form a part of the thesis as well.

KEYWORDS

Information Systems, Assessment of Information Systems, Deficiencies in Operation and Management of Information Systems, Security of Information Systems, Audit of Information Systems, Case Study, IT Governance

BIBLIOGRAFICKÁ CITACE

NOVÁK, Lukáš. *Metodika hodnocení informačních systémů*. Dizertační práce. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 125 s. Vedoucí práce: doc. Ing. Miloš Koch, CSc.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená dizertační práce s názvem Metodika hodnocení informačních systémů je původní a zpracoval jsem ji samostatně pod vedením mého školitele. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně, dne 18. října 2017 …….

Ing. Lukáš Novák

PODĚKOVÁNÍ

Děkuji především vedoucímu své dizertační práce doc. Ing. Miloši Kochovi, CSc. za metodické vedení, odbornou pomoc, nadhled, nikdy neodcházející optimismus a cenné rady a náměty pro vytvoření konečné podoby dizertační práce. Dále děkuji své rodině za podporu a poskytnuté zázemí. V neposlední řadě patří upřímný dík všem, kteří se, a třeba jen malinko, zasloužili o to, aby tato práce vznikla. Moc děkuji!

OBSAH

1 ÚVOD A CÍL PRÁCE

Společně s vývojem nových technologií se rozsah použití informačních a komunikačních systémů rozšiřuje. Dnešní technologie jsou všudypřítomné a nabízejí celou řadu nových možností použití. Každá nová inovace a její oblast aplikace představuje nové výzvy i v případě měření a vyhodnocování výsledků.

Svět informačních a komunikačních technologií se rychle mění. Mnoho současné literatury odkazuje na doby, kdy bylo hodnocení informačních systémů relevantní pouze pro společnosti, které zaváděly informační systém vyvinutý vlastními silami. Dnešní systémy přesahují hranice firmy a přidávají tak nový ekonomický pohled na dělení výdajů a přínosů. Díky dominanci internetu a webových systémů je možné pozorovat v současném řízení informatiky více subjektů než dříve. Nezřídka je vývoj a provoz systémů zajišťován externě. Jedním z problémů, které řeší manažeři firem, je ocenění hodnoty informačních a komunikačních technologií. Management totiž investuje do nových systémů nemalé prostředky, aby snížil náklady a podnik zůstal konkurenceschopný. Nicméně velmi často neexistují hmatatelné důkazy o přidané hodnotě. Navíc se firma musí vypořádat s nálezy procesního či finančního auditu, které vznikly zavedením nových systémů. Nápravná opatření jsou obvykle časově i finančně náročná.

Globalizace spolu s rozvojem informačních a komunikačních technologií měla obrovský dopad na způsob fungování firem. Tento vývoj neustále ovlivňuje strategie, taktiky a operativní rozhodování organizací. Informační systémy umožňují zahájení nových služeb v rámci firmy i podnikání mezi organizacemi a jsou považovány za klíčové pro účinnost a efektivitu moderního podnikání. Tento argument dříve omlouval vysoké investice, které podnik vynaložil, aby udržel konkurenční výhodu na globálním trhu. Z dnešního pohledu byl ale překonaný, protože jsou tyto systémy často zapotřebí jen proto, aby podnik mohl být provozuschopný. Z velké části jsou investice motivovány potřebou dodat lepší hodnotu výrobků a služeb prostřednictvím robustních dodavatelských řetězců. Navzdory stále rostoucím investicím do infrastruktury a aplikací nejsou eliminovány nedostatky pramenící z používání informačních systémů. Naopak jsou spíše stále rozšiřovány. A to přes existenci mnoha výzkumů na toto téma i existenci nových metodik a frameworků. Proto je význam hodnocení stavu IS/ICT stále aktuálním tématem v rámci organizace i předmětem nových výzkumů.

S vývojem informačních technologií vzrostlo povědomí o strategickém významu informací. Současně se také přizpůsobovala pozice informatiky v organizační struktuře firem a cíle řízení informačních systémů. Tento vývoj vedl k definování informační strategie, která má představu o tom, jak budou cíle spojené s IS/ICT dosaženy. V souladu se strategií a finančním plánováním rostou obavy manažerů také v oblasti bezpečnosti. Jakýkoli nedostatek totiž může mít velmi negativní dopad na chod celé organizace. Dalším důležitým tématem, který je akcentován především u středních a větších firem, je soulad s normami, zákony či požadavky auditů. Negativní výrok může mít totiž vliv na konkurenceschopnost firmy.

Dizertační práce se zaměřuje na hodnocení informačních systémů, které je důležitým tématem pro studium i praxi. Když se informační systémy staly všudypřítomné a v některých podnicích dokonce nenahraditelné, metody pro hodnocení se dle Lagstena (2011) do jisté míry změnily. V současné době autoři metod začali zjišťovat, do jaké míry a jak firmám informační systémy a informatika obecně slouží. Jedním z hlavních důvodů pro hodnocení informačních systémů je získat zpětnou vazbu a přijmout opatření na základě výsledků. Ačkoli je v této oblasti značné množství zejména zahraniční literatury, nadále existují rozdíly v uplatňování výsledků výzkumu.

Rychlý růst investic do oblasti informačních systémů přináší tlak na management, který musí brát v úvahu investiční rizika. Komplexní a srozumitelná metodika je nutná pro hodnocení informačních systémů, jejichž složitost plyne z heterogenity nových přístupů a technologií. Výběr správného řešení a snížení rizik může být klíčovým faktorem pro udržení životaschopnosti a prosperity firmy. Finanční manažeři mohou používat různé metody pro hodnocení nákladů a přínosů, a to od jednoduchých výpočetních vzorců až po velmi složité techniky, v nichž se snoubí kvantitativní a kvalitativní analýzy do jednoho ukazatele. Zmíněné metody se používají především pro investiční rozhodování, ale nemusí vždy zachytit všechny dopady zaváděných technologií. Potíže s odůvodněním investic do nápravných opatření jsou spojeny s nehmotnou povahou přínosů. Jedná se například o nastavení formalizovaného procesu změn přístupových oprávnění nebo změny ve změnovém řízení. Samotný proces hodnocení by však neměl být příliš složitý. A pokud je, stává se použití metodiky kontraproduktivní. Proto je nutné použít přístup, který bude produkovat dostatečné výhody, aby si zasloužil čas a úsilí manažerů.

1.1 Cíl práce

Cílem dizertační práce je **navržení vlastní metodiky pro hodnocení informačních systémů**. Předpokladem nové metodiky je navázat na předchozí výzkum a inovovat současné postupy a metodiky.

Mezi dílčí kroky, které je třeba učinit k dosažení cíle, se řadí určení technik a identifikování hlavních kritérií, která by měla být brána v úvahu při hodnocení informačních systémů. Dále je nutné provést rešerši informačních zdrojů, analyzovat současný stav problematiky, realizovat primární výzkum pomocí hloubkových rozhovorů, vyhodnotit získaná data, vytvořit metodiku hodnocení informačních systémů a verifikovat ji kvalitativním přístupem pomocí případových studií.

Vyhodnocením cíle práce se zabývá samostatná kapitola 4.6.1.

1.2 Formulace výzkumných otázek

Výzkumná otázka představuje základní východisko vědecké práce. Výzkumná otázka dle Strausse a Corbinové (1999, s. 24) definuje, co je zapotřebí zodpovědět, aby se dosáhlo cíle.

V souladu s oblastí výzkumu, která je zaměřená na vytvoření metodiky hodnocení informačních systémů, představují výzkumný problém nedostatky v oblasti provozu a řízení informačních systémů. Účelem výzkumu je nedostatky identifikovat a navrhnout opatření. První výzkumná otázka pro účely této dizertační práce je stanovena následovně:

VO1: Jaké jsou hlavní nedostatky v oblasti provozu a řízení informačních systémů a možná opatření vedoucí k jejich odstranění?

V souladu s cílem práce a první výzkumnou otázkou je stanovena druhá výzkumná otázka zaměřující se na použití vytvořené metodiky hodnocení informačních systémů v praxi v kategorii malých, středních a velkých firem následovně:

VO2: Jaké nedostatky v provozu a řízení informačních systémů je možné odhalit při použití navrhované metodiky v praxi v malé, střední a velké společnosti?

Vyhodnocením výzkumných otázek se zabývá samostatná kapitola 4.6.2.

1.3 Harmonogram

V následující kapitole je uveden harmonogram zpracování dizertační práce. Součástí je vymezení všech nezbytných úkonů, které bylo nutné realizovat pro splnění cíle práce.

2012 Zahájení doktorského studia, stanovení tématu dizertační práce.

Studium literatury (VUT v Brně / Nottingham Trent University).

Publikace článku, který se zabývá srovnáním přístupů hodnocení informačních systémů (Novák, 2012).

2013 Zpracování literární rešerše (VUT v Brně / Technische Universität Wien).

Definování cíle a postupných kroků pro splnění cíle dizertační práce.

Publikace článku zabývající se výdaji na informační systémy a technologie ve firmách v České republice (Novák, 2013).

Stanovení výzkumných otázek dizertační práce.

Identifikace vědeckých metod pro provedení výzkumu.

Zpracování pojednání ke Státní doktorské zkoušce.

2014 Publikace článku zabývající se analýzou vlivu vývoje ekonomiky na výdaje a investice v IT v České republice, Polsku, Slovensku a Maďarsku (Novák, 2014a).

Publikace případové studie zabývající se faktory úspěšnosti (Novák, 2014b).

Příprava hloubkových rozhovorů.

2015 Úspěšné složení Státní doktorské zkoušky.

Ověření metodických postupů, aktualizace literární rešerše.

Provedení hloubkových rozhovorů s odborníky.

Publikace případové studie zabývající se identifikací nedostatků v oblasti provozu a řízení informačních systémů a návrhem změn (Novák, 2015a).

Publikace článku, jehož cílem bylo porovnat vytvořené metodiky pro hodnocení informačních systémů (Novák, 2015b).

2016 Vyhodnocení hloubkových rozhovorů.

Vytvoření a testování vlastní metodiky hodnocení informačních systémů.

Publikace článku popisující návrh vlastní metodiky pro hodnocení informačních systémů (Novák, 2016).

2017 Analýza, hodnocení a formulování výsledků.

Zodpovězení výzkumných otázek a vyhodnocení stanoveného cíle.

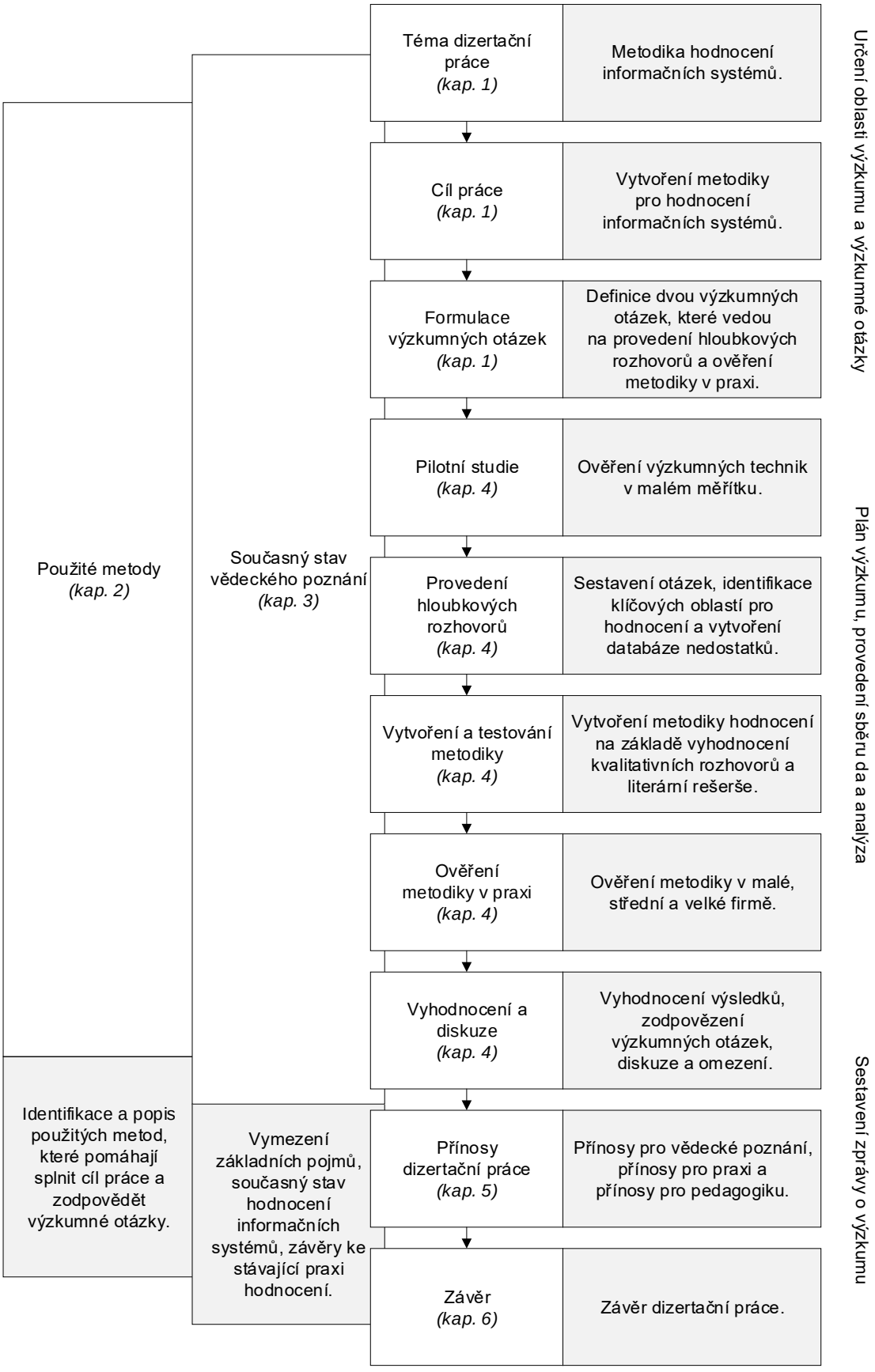
1.4 Postup zpracování

Výzkum prezentovaný v této dizertační práci se sestává ze tří po sobě jdoucích kroků: určení oblasti výzkumu a výzkumné otázky, návrh plánu výzkumu, provedení sběru dat a jejich analýza a sestavení zprávy o výzkumu. Všechny zmíněné kroky zobrazuje obrázek č. 1, který slouží jako osnova pomáhající udržet systém a logickou návaznost mezi jednotlivými kroky výzkumu a souvisejícími kapitolami dizertační práce. Graficky je zde znázorněno, že použité metody a současný stav vědeckého poznání prochází všemi výzkumnými kroky a slouží jako jeden ze základních kamenů práce. Výzkumný proces začíná definováním tématu práce a cíle práce. V souladu s výzkumnými otázkami byly následně provedeny a vyhodnoceny hloubkové rozhovory. Dále navazuje stěžejní fáze zaměřená na vytvoření metodiky, její testování a ověření v praxi. Díky získaným výsledkům bylo možné zodpovědět výzkumné otázky a formulovat přínosy práce.

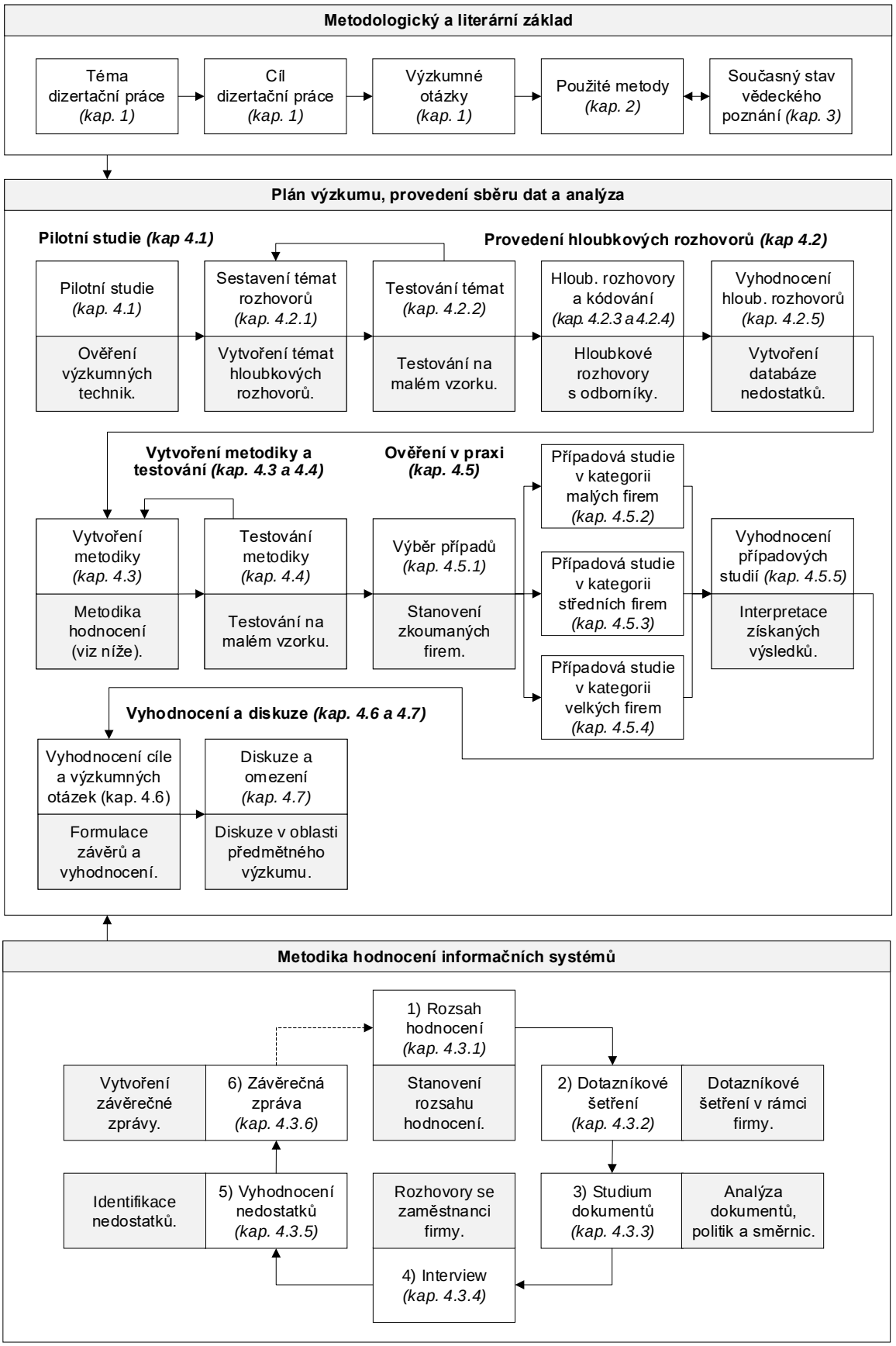
Fáze Plán výzkumu, provedení sběru dat a analýza je dále rozpracována na obrázku č. 2, ve kterém je detailně naznačen každý krok výzkumného procesu včetně krátkého vysvětlení. Grafika na obrázku navazuje na definici výzkumných otázek z obrázku č. 1 a rozpracovává všechny kroky až po bod týkající se zodpovězení výzkumných otázek. Vše znovu vychází z metodologického a literárního základu, který slouží jako pomocný bod ovlivňující všechny kroky výzkumu.

Provedení hloubkových rozhovorů se skládá z několika kroků. Nejdříve byla sestavena a na malém vzorku otestována témata, následně byly provedeny rozhovory s odborníky a pomocí kódování vyhodnoceny. Na jejich základě byla sestavena metodika hodnocení informačních systémů skládající se ze šesti následujících fází: rozsah hodnocení, dotazníkové šetření, studium dokumentů, interview, vyhodnocení nedostatků a závěrečná zpráva. Metodika byla nejdříve otestována na malém vzorku a poté byla v souladu s druhou výzkumnou otázkou ověřena kvalitativním přístupem pomocí případových studií v malé, střední a velké společnosti. V další fázi byly na základě dílčích výsledků sestaveny výsledky celého výzkumu.

Postup zpracování výzkumu koresponduje s autory metodologických příruček, jako je například Liška (2004), Punch (2008), Reichel (2009), Disman (2011), Molnár (2011 a 2012), Široký (2010 a 2011) nebo Hendl (2016).



Obrázek 1: Postup zpracování dizertační práce



Obrázek 2: Detailní rozpracování fáze Plán výzkumu, provedení sběru dat a analýza

1.5 Organizace dizertační práce

Dizertační práce je rozdělena do šesti hlavních kapitol. Úvodní kapitola se zaměřuje na stanovení cíle dizertační práce, odůvodnění vybraného tématu a postupu zpracování. Nedílnou součástí je také formulace výzkumných otázek.

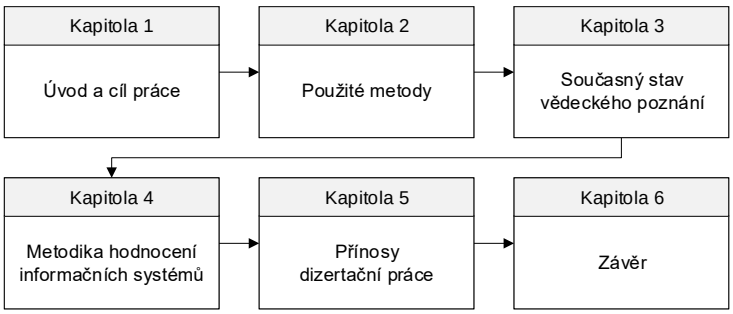
Druhá kapitola byla vyhrazena použitým vědeckým metodám. Jedná se o identifikaci a popis použitých metod v dizertační práci, které vedou ke splnění cíle práce, logicky roztříděných do dvou podřízených částí.

Třetí kapitola čítá základní teoretická východiska, která se odvíjí od tématu práce. Text první části kapitoly systematicky postupuje od vysvětlení základních pojmů až k popisu komplexních oblastí. Samostatná kapitola byla věnována rešerši, která dle Širokého (2011, s. 15) představuje vyhledávání, pátrání či výzkum s cílem získat informace v předmětné oblasti zájmu. Nejedná se však o vyčerpávající popis celé oblasti informačních systémů, v textu je věnována především pozornost základním trendům. Poté následuje souhrn současného stavu ve výzkumu i praxi. Tato sumarizace pomohla k odhalení nedostatků i vytvoření metodiky, kterou pokrývá tato práce.

Čtvrtá kapitola přichází se samotným výzkumem vedoucím k nalezení všech podkladů pro zpracování řešeného problému. Součástí je pilotní studie, primární výzkum pomocí hloubkových rozhovorů, návrh nové metodiky a její ověření v praxi i vyhodnocení cílů a formulace odpovědí na výzkumné otázky.

Pátá kapitola je věnována přínosům dizertační práce, které jsou formálně členěny do tří samostatných částí.

Závěr dizertační práce je zpracován v šesté kapitole.



Obrázek 3: Organizace dizertační práce

2 POUŽITÉ METODY

Kapitola použitých metod je rozdělena do několika částí. V první podkapitole jsou definovány použité metody vědeckého zkoumání, ve druhé části se práce zaměřuje na metody sběru dat a třetí pojednává o použitých metodách vyhodnocení a interpretace.

V rámci dizertační práce jsou použity pojmy **metodologie**, **metoda** a **metodika**, jejichž vztah je rozklíčován v tomto odstavci. Rozdíl mezi metodologií a metodou výstižně uvádí Hendl (2016, s. 32–33) či Široký (2011, s. 27–29). Metodologie je nauka o metodách, které lze při vědecké práci používat. Vědecká metoda je systematickým, promyšleným a objektivním postupem k získání poznatků a dosažení cíle. Metodika podle Širokého (2011, s. 28) definuje konkrétní postup řešení určitého problému a představuje určitý návod, jak dosáhnout cíle.

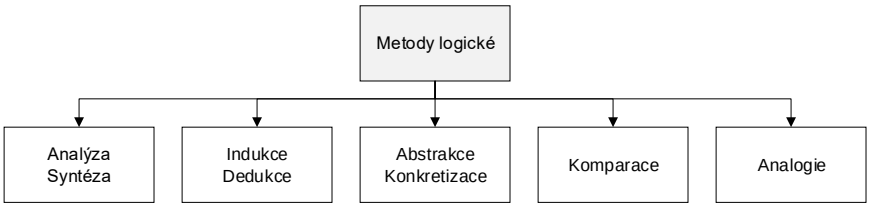
Při zpracování dizertační práce byl aplikován **systémový přístup**, kdy se na formulaci problému, jeho pojetí i interpretaci výsledků nahlíží komplexně. Jak uvádí Dostál a kol. (2005, s. 17) nebo Rais a Doskočil (2011, s. 12), systémovým přístupem označujeme takový způsob myšlení, řešení úloh a jednání, při němž jsou jevy chápány v jejich vnitřních i vnějších souvislostech. Systém lze podle Janíčka a Marka (2013, s. 41) definovat jako účelově definovanou neprázdnou množinu prvků a množinu vazeb mezi nimi, přičemž vlastnosti prvků a vazeb mezi nimi určují vlastnosti celku. Pro takový systém pak identifikujeme podle Molnára (2012, s. 68–69) především účel systému, strukturu systému, vlastnosti prvků, vlastnosti vazeb, okolí systému a případné subsystémy. V rámci dekompozice systému lze vyjmout podsystém, který představuje podmnožinu systémových prvků a vazeb, které jsou vyčleněny ze systému a jsou chápány jako nový systém nebo jako prvek. Prvek je část systému, který tvoří na dané rozlišovací úrovni dále nedělitelný celek, jehož strukturu nechceme nebo již nemůžeme rozlišit. Rozlišovací úrovní se označuje stupeň podrobnosti zkoumání systému. Dekompozicí systému na jednodušší prvky se zvyšuje rozlišovací úroveň. Systémová integrace je podle Svozilové (2016, s. 49) kombinací systémů a jejich částí do jednotlivého a funkčního technologického celku při zachování všech procesních potřeb uživatele nebo skupiny uživatelů systému.

2.1 Metody vědeckého zkoumání

Vědecké postupy můžeme klasifikovat podle různých hledisek. Možné dělení je založeno na způsobu vysvětlení zkoumaného problému. Na základě tohoto kritéria pak vymezujeme typy vědeckých metod, ke kterým patří dle Ochrany (2013, s. 100) metody **explanační** a **interpretační**. Autor dále uvádí, že při explanaci postupujeme od obecného k jednotlivému. Obecným je známý vztah a jednotlivým je vysvětlovaný jev, který zařazujeme pod daný obecný vztah. Naproti tomu interpretační metoda se zakládá na pochopení, nikoli vysvětlení. Rozdělení vědeckých metod i kritéria dělení jsou nepatrně odlišné u různých autorů. Mezi nejčastěji uváděné, např. u Molnára (2012, s. 40–41), nebo Širokého (2011, s. 29–30), patří dělení na metody logické a empirické. Těmto metodám je věnována první a druhá podkapitola. Modelování, jako další vědecké metodě, se věnuje třetí podkapitola.

2.1.1 Metody logické

Logické metody jsou založeny na využívání principu logického myšlení. Podle Hendla (2016, s. 32–34) nebo Molnára (2011, s. 9) k nim patří: analýza a syntéza, indukce a dedukce a abstrakce a konkretizace. V literatuře bývají také označeny jako párové metody. Široký (2011, s. 29) k nim dále ještě řadí komparaci a analogii.



Obrázek 4: Klasifikace logických metod (Široký, 2011 a Molnár, 2012)

Analýza dle Hendla (2016, s. 32) spočívá v rozdělení celku na komponenty a následném zkoumání, jak tyto komponenty fungují jako samostatné prvky a jaké jsou mezi nimi vztahy. Podle Širokého (2011, s. 31) jde o myšlenkové rozložení zkoumaného jevu na dílčí složky, které se stávají předmětem dalšího bádání. Opakem analýzy je **syntéza**, která podle Molnára (2011, s. 9) znamená postupovat od části k celku a dovoluje poznávat objekt jako jediný celek. V dizertační práci byla analýza použita při zkoumání vědeckých pramenů, které se zabývají problematikou hodnocení informačních systémů. Syntéza byla použita při sestavování souboru kritérií pro hodnocení informačních systémů.

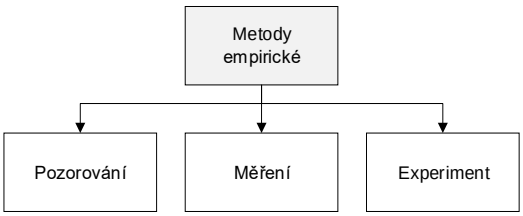
Indukci definuje Molnár (2011, s. 9) jako postup od zvláštního k obecnému. Indukce je proces vyvozování obecného závěru na základě poznatků o jednotlivostech. Hendl (2016, s. 34) definuje **dedukci**, která je s indukcí silně spjata, jako logické odvození závěru z množiny jiných tvrzení. Využití indukce v dizertační práci lze spatřovat při zobecňování poznatků získaných ve vlastním výzkumu. Metoda dedukce byla průběžně používána v procesu zpracování dizertační práce. Například byla uplatněna při využití informací získaných z odborných publikací.

Abstrakce je dle Ochrany (2013, s. 37) metoda, při níž se oddělují nepodstatné a nahodilé vlastnosti zkoumaného jevu. **Konkretizace** je opačný proces, kdy vyhledáváme konkrétní výskyt určitého objektu z určité třídy objektů a snažíme se na něj aplikovat charakteristiky platné pro tuto třídu objektů. Abstrakce byla použita pro účely identifikace důležitých faktorů pro hodnocení informačních systémů. Konkretizace byla použita například při identifikaci jednotlivých nedostatků v rámci hodnocení informačních systémů.

Komparace je dle Reichla (2009, s. 28) postavena na principu srovnávání jistých vlastností u zvolených předmětů zkoumání. Při srovnání se určují shodné či rozdílné stránky různých jevů nebo předmětů. **Analogii** definuje Široký (2011, s. 33) jako proces hledání či nalezení totožného vztahu mezi zkoumanými jevy a objekty. Komparace i analogie byly použity při srovnávání metodik v rešeršní fázi dizertační práce.

2.1.2 Metody empirické

Oproti teoretickému výzkumu, který je založen na dedukci, analýze a komparaci pojmů, empirický výzkum, jak uvádí Reichel (2009, s. 32), operuje s konkrétními údaji o jevech a procesech. Empirické metody pracují s daty a exaktními metodami a dospívají ke konkrétním poznatkům. Řadí se k nim dle Širokého (2011, s. 15) pozorování, měření a experiment.



Obrázek 5: Klasifikace empirických metod (Široký, 2011)

Pozorování je podle Reichla (2009, s. 94) definováno jako technika sběru informací založená na zaměřeném, systematickém a organizovaném sledování smyslově vnímatelných projevů aktuálního stavu prvků, aspektů nebo fenoménů. Opakováním pozorování lze dosáhnout větší korektnosti metody, neboť se minimalizuje náhodná složka. Pozorování bylo využito jako vědecká metoda v mnoha částech práce, především v rámci formulování metodiky pro hodnocení informačních systémů.

V rámci metody **měření** se dle Širokého (2011, s. 36) provádí kvalitativní srovnání určitých vlastností srovnatelných jevů a objektů. Měření bylo v práci využito při vyhodnocování rozhovorů a dotazníků pomocí popisné statistiky.

Základní vlastností **experimentu** je podle Hendla (2016, s. 44) to, že výzkumník aktivně a úmyslně přivodí určitou změnu situace, okolnosti nebo zkušenosti sledovaných jedinců a pak sleduje změnu jedinců. Tímto způsobem se výzkumník pokouší vytvořit zjednodušený model skutečnosti, aby se co nejvíce podobal realitě. Metoda byla použita v rámci testování navrhované metodiky hodnocení informačních systémů.

2.1.3 Modelování

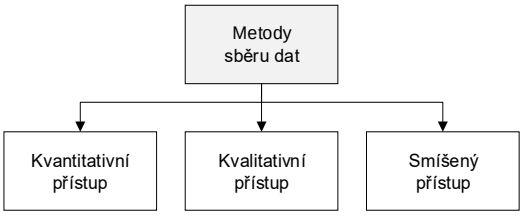
Model systému představuje podle Dostála (2008, s. 5–7) zjednodušené zobrazení reality, na kterém se dají studovat vlastnosti, které jsou z hlediska studovaného jevu významné. **Modelování** lze charakterizovat jako proces projektování a konstrukce modelu. Podle Širokého (2011, s. 33) představuje modelování metodu, která prostřednictvím formulace problému, vytváření modelu a výzkumu modelu přenáší znalost o modelu zpět na realitu. Model lze potom chápat jako účelné a zjednodušené znázornění zkoumaného systému, přičemž model se shoduje s originálním systémem v podstatných vlastnostech.

Modely lze dle Raise a Doskočila (2011, s. 16) klasifikovat podle následujících tří hledisek. Rozdělení na deterministické a stochastické modely charakterizuje povaha vztahů mezi veličinami, dle kritéria času je možné dělit na statické a dynamické modely a dle míry seskupení na mikroekonomické a makroekonomické modely.

Metoda modelování byla použita v dizertační práci v rámci návrhu metodiky pro hodnocení informačních systémů.

2.2 Metody sběru dat

Metody sběru dat lze členit dle odlišné strategie k provádění výzkumu na kvantitativní a kvalitativní. Základním rozdílem mezi těmito dvěma přístupy, jak uvádí Molnár (2012, s. 44–47), je způsob poznání. Logika kvantitativního výzkumu je deduktivní, a naopak logika kvalitativního výzkumu induktivní. V kvantitativním výzkumu je získán obecný rozsah informací o velice mnoha jedincích, zatímco v kvalitativním výzkumu je získáno mnoho informací o velmi malém počtu jedinců. Reichel (2009, s. 42) ale dodává, že oba přístupy jsou si navzájem rovnocenné a doplňují se.



Obrázek 6: Metody sběru dat (Široký, 2011)

Kvantitativní přístup podle Reichla (2009, s. 40) předpokládá, že objekty zkoumání jsou měřitelné nebo tříditelné a uspořádatelé. Kvantitativní výzkum spočívá dle Molnára (2012, s. 44–45) v analýze dat, která mohou být získána buď přímým pozorováním, nebo dotazováním. Široký (2011, s. 64–65) řadí mezi techniky kvantitativního výzkumu pozorování, dotazník, rozhovor, studium dokumentů a experiment.

Kvalitativní přístup představuje řadu rozlišných postupů, které se snaží porozumět zkoumanému problému. Cílem je nahlížet na určitý fenomén v co možná nejkomplexnější podobě včetně vztahů k dalším aspektům. Hendl (2016, s. 45–51) dodává, že v kvalitativní metodě je možno modifikovat nebo doplňovat otázky v průběhu výzkumu. Práci kvalitativního výzkumníka přirovnává k práci detektiva, který se seznamuje s novými lidmi, pracuje v terénu. Sběr dat a jejich následná analýza většinou zabere delší časový interval. Široký (2011, s. 71–72) mezi nejčastější techniky kvalitativního přístupu řadí: hloubkové interview, nestandardizované pozorování a analýzu obsahu.

Smíšený výzkum představuje dle Hendla (2016, s. 58) postup využívající obou strategií. V rámci tohoto přístupu se použijí kvalitativní i kvantitativní postupy obvykle ve zmíněném pořadí.

2.2.1 Dotazníková metoda

Dotazník se podle Širokého (2011, s. 66) řadí k nejrozšířenějším metodám pro získávání dat. Autor dále uvádí, že dotazníky jsou určeny k usnadnění komunikace mezi výzkumným pracovníkem a respondentem a poskytují větší čas na promyšlení odpovědi.

V dotazníku se mohou objevit podle Kozla (2011, s. 213) následující typy otázek: otevřené, polouzavřené a uzavřené. Při použití **otevřených otázek** je možná volná volba odpovědi. Respondent reaguje vlastními slovy a není omezován. Mezi nevýhody se řadí složitější zpracování získaných dat. U **polouzavřených otázek** jsou rozpracovány všechny odpovědi na otázku včetně poslední varianty, která nabízí možnost vyjádřit vlastní názor v případě, že ostatní odpovědi nevyhovují. **Uzavřené otázky** přestavují vyčerpávající soubor všech možných odpovědí, které se musí navzájem vylučovat. Široký (2011, s. 68) uvádí mnoho variant uzavřených otázek: dichotomické (výběr ze dvou možností), výběrové (výběr jedné alternativy), výčtové (výběr více alternativ), vylučovací (výběr alternativy, která je vyloučena), stupnicové (určení pořadí), komparativní (kombinace výčtové a stupnicové), filtrační (eliminuje respondenty, kteří nemají k tématu co říci), nepřímé (dotaz je směřován jako názor celé skupiny), kontrolní (ověřují věrohodnost) a projekční (dotazuje se na názory jiných osob).

Dotazník byl v dizertační práci vytvořen na základě analýzy výsledků hloubkových rozhovorů a literární rešerše. Je použit v mnohonásobné případové studii k odhalení nedostatků v oblasti informačních systémů. V dotazníku byly použity uzavřené otázky výběrové, trichotomické a v několika případech i kontrolní.

2.2.2 Hloubkové rozhovory

Hloubkové rozhovory se snaží zachytit hlubší příčiny určitých názorů či chování. Tazatel jasně sestavenými otázkami pobízí respondenta k formulování vlastních odpovědí. Ty jsou poté dotazovaným zpracovány a vyhodnoceny. Průběh rozhovoru se může lišit dle Hendla (2016, s. 168–195) v mnoha pohledech. **Standardizovaný rozhovor** vypadá jako předčítání dotazníku respondentovi, který odpovídá na předem zvolené varianty odpovědí. **Hloubkový rozhovor** pak připomíná volný rozhovor, jehož struktura není pevně dána. Mezi další možnosti patří strukturovaný otevřený rozhovor, rozhovor

s návodem, neformální rozhovor, fenomenologický rozhovor, narativní rozhovor, epizodické interview a skupinová diskuze. Jednotlivé přístupy se liší mimo jiné přípravou, počtem osob i formou dotazování.

Rozhovor pomocí návodu byl použitý při úvodní fázi výzkumu, jehož cílem bylo identifikovat kritéria sloužící pro hodnocení informačních systémů. Návod byl sestaven na základě pilotní studie a současného stavu vědeckého poznání. Přestože se postupuje podle návodu, nezáleží na pořadí, ani na přesném znění otázek. Tazatel si je může přizpůsobit.

V rámci navrhované metodiky hodnocení informačních systémů byl také použitý rozhovor pomocí návodu. Návod byl sestaven na základě domén a kategorií vzešlých z hloubkových rozhovorů zmíněných v předchozím odstavci a následným uspořádáním oblastí do vhodného pořadí.

2.2.3 Případová studie

Případová studie se dle Hendla (2016, s. 102) zabývá intenzivním studiem jednoho nebo několika případů. Případové studie vysvětlující problémy a jevy jak v minulosti, tak i v současnosti, které se děly nebo dějí v jedné organizaci či v celé skupině organizací. Jedná se na rozdíl od kvantitativních přístupů o sběr velkého množství dat od jednoho nebo několika jedinců. Jde o zachycení složitosti případu a o popis vztahů jejich celistvosti. Případová studie začíná výzkumnou otázkou a končí vřazením zkoumaného případu do širších souvislostí, v případě potřeby ho lze srovnat s jinými případy.

Hendl (2016, s. 103) rozlišuje typy případových studií na studii **osobní**, **komunity**, **sociálních skupin**, **organizace** a **zkoumání programů, událostí, rolí a vztahů**. Osobní studie se zabývá zkoumáním aspektu u jedné osoby, studie komunity zkoumáním komunit a studie sociálních skupin sleduje malé skupiny. Studie organizace se zabývá zejména evaluací a výzkumem firemních procesů a zkoumání programů či událostí se zaměřuje na určitou událost. V dizertační práci byla využita případová studie zabývající se studiem organizací.

Podle Yina (2012, s. 167) lze případové studie dělit na **explorační**, **explanatorní, deskriptivní** a **evaluační**. Explorační má za cíl prozkoumat neznámou strukturu případu a působící vztahy. Explanatorní studie podává vysvětlení případu tím, že rozvádí

jednotlivé příčinné řetězce, které lze u případu identifikovat. Deskriptivní případová studie podává kompletní popis jevu a evaluační provádí popis, explanaci nebo exploraci s cílem hodnocení na základě definovaných kritérií. V dizertační práci byla využita evaluační případová studie jako nástroj pro ověření navrhované metodiky hodnocení informačních systémů v praxi.

Dále lze dělit případové studie podle Staka (1995, s. 3–4) na **intrinsitní**, **instrumentální** a **kolektivní**. Intrinsitní případová studie se do hloubky věnuje jedinému případu. Instrumentální se zabývá případy obecnějšího jevu, kde je po zvolení jevu vyhledán případ, který tento jev reprezentuje. Kolektivní případová studie, která se využívá v komparativních výzkumech, zkoumá více instrumentálních případů. Kolektivní případovou studii, kterou rozeznává Stake (1995, s. 25), detailněji popisuje i Yin (2012, s. 8) jako mnohonásobnou případovou studii. Yin (2012, s. 17) dále definuje u mnohonásobných případových studií strategie replikace. Případová studie podle zmíněného přístupu představuje samotnou studii, která se dobírá určitých závěrů majících vztah k samotnému případu. Tyto informace se stávají podkladem pro jeho replikaci ostatními případy. Logika replikace je buď literární nebo teoretická. Pokud se pracuje ve výzkumu s podobnými případy, u nichž je možné předvídat stejné výsledky, jde o literární replikaci. U teoretické replikace se pracuje s velmi rozdílnými případy, které vedou k rozdílným výsledkům. Souhrnná zpráva obsahuje zprávy o jednotlivých případech a celkové zhodnocení včetně komparace. Plán provedení mnohonásobných případových studií je dle Yina (2012, s. 17–18) a Staka (1995, s. 54) následující:

- definice a plán výzkumu (identifikace objektu výzkumu, zvolení studovaných jevů a definice výzkumné otázky),
- příprava, sběr dat a analýza (hledání pravidelnosti v datech se vztahem k výzkumné otázce, doplnění klíčového pozorování a datového základu),
- analýza a závěry (identifikace alternativních interpretací, návrh základního tvrzení a zobecnění pro daný případ).

V dizertační práci byla v rámci ověření navržené metodiky využita mnohonásobná případová studie, která zkoumá několik vybraných firem.

2.2.4 Analýza dokumentů

Analýza obsahu dokumentů patří ke standartní aktivitě výzkumu a slouží jako doplňující technika či informační zdroj. Pro výzkumné účely se dle Hendla (2016, s. 208) používají dokumenty, které vznikly v minulosti a byly pořízeny někým jiným než výzkumníkem, a pro jiné účely, než jaký má aktuální výzkum. Jsou to tedy již existující dokumenty, které mohou mít různou podobu. Tato technika se hodí pro doplnění nebo verifikaci platnosti poznatků získaných jinou cestou. K výhodám se řadí fakt, že **data nejsou zkreslená**, tak jako u interview. Subjektivita výzkumníka hraje roli při výběru dokumentů, nikoli v informacích, které jsou v dokumentech. Při samotné analýze dokumentů je možné postupovat obdobně jako u analýzy rozhovorů. Hendl (2016, s. 135) dále posuzuje dokumenty podle šesti kritérií: typ dokumentu, vnější znaky dokumentu (stav dokumentu a jeho zpracování), zkoumání vnitřních znaků dokumentu (analýza obsahu), intencionalita dokumentu, blízkost dokumentu k předmětu zkoumání či časová blízkost a původ dokumentu (např. autor dokumentu).

V dizertační práci bude tato technika použita pro analýzu interních dokumentů, předpisů a směrnic firmy vztahující se zejména k informačním systémům a IT oddělení firmy.

2.2.5 Metoda triangulace

Metoda triangulace se používá při kombinaci různých vědeckých metod. V triangulaci jde dle Molnára (2012, s. 47–48) o paralelní užívání různých druhů dat či různých metod při studiu jednoho a téhož problému. Cílem triangulace je zkrátka očistit spolehlivé informace od nespolehlivých, získat validní a objektivní obraz studovaného objektu. Hendl (2016, s. 151–152) rozlišuje různé typy triangulací: triangulace **datová** (použití různých datových zdrojů), **výzkumníků** (využití více tazatelů či pozorovatelů) a **metodologická** (kombinace metod). S triangulací je silně spojená smíšená strategie výzkumu, která právě kombinuje kvalitativních a kvantitativních přístupy. V rámci této strategie se užívá kombinace několika technik, a to především proto, aby se dosáhlo vyšší validity výsledků. Cílem je řešit komplexnější výzkumné otázky a eliminovat slabé a využít silné stránky obou přístupů.

Při vyhodnocování výsledku navrhované metodiky, která kombinuje dotazník, studium dokumentů a interview, byla využita metodologická triangulace.

2.3 Metody vyhodnocení a interpretace dat

U kvantitativního výzkumu je návaznost činností souvisejících se sběrem a analýzou dat pevně nastavena. Nejdříve probíhá sběr dat a poté následuje jejich analýza. Kvalitativní přístup umožňuje začít v některých případech s organizováním a třízením dat už ve fázi sběru dat. Způsoby třízení a vyhodnocování dat jsou velmi různorodé, v této práci jich bylo použito hned několik. Jedná se především o metodu kódování, metody spjaté s vyhodnocováním případové studie a statistickou analýzu. Na detailní vyhodnocení dat navazuje interpretace dat, která je spjata s výzkumnou zprávou. Jejím cílem je informovat čtenáře o tom, co se zkoumalo a k jakým výsledkům výzkumník dospěl. **Výzkumná zpráva** má podle Hendla (2016, s. 339–440) také za úkol vysvětlit, čím se výzkum zabýval, informovat o prostředí, ve kterém se prováděl, jakým způsobem byl výzkum proveden, měl by obsahovat základní informace a formulaci závěrů.

2.3.1 Metoda kódování

Kódování definuje Reichel (2009, s. 164–167) jako rozčlenění množin a souborů údajů na dílčí celky, segmenty a jejich následné pojmenování a třídění. To se během analýz několikrát opakuje a zpřesňuje. Pokud vyhodnocení materiálu a jeho další sběr nic nového nepřinášejí, lze dosáhnout teoretické saturace a výzkum může být ukončen.

V rámci kvalitativního výzkumu se pracuje s daty, které mají nejčastěji formu textu a zahrnují mimo jiné přepisy rozhovorů nebo audiovizuálních nahrávek. Jedná se o velké množství nestrukturovaného materiálu, se kterým je nutné dále pracovat. Základním způsobem, jak analyzovat tato neuspořádaná data je otevřené kódování.

Otevřené kódování probíhá při prvních analýzách údajů, tvoří kategorie a identifikuje základní oblasti. Jedná se o analytickou techniku, která byla vyvinuta v rámci zakotvené teorie podle Strausse a Corbinové (1999, s. 42–43). Otevřené kódování je počátečním krokem kvalitativní analýzy dat, které směřuje k velmi detailní a hloubkové práci s textem. Hendl (2016, s. 251) uvádí, že při otevřeném kódování výzkumník analyticky pročítá text, hledá v něm témata a rozděluje ho na dílčí jednotky. Hranice členění výzkumník volí podle významu informace. Některé části textu obsahují více informací, proto se mohou hranice některých významových jednotek překrývat. Každé významové

jednotce je následně přiřazen kód, který vystihuje obsah analyzovaného textu. V případě, že jednotka bude reprezentovat více než jedno téma, pak je možné ji označit více kódy. Rozdělení textu na segmenty a jejich zakódování umožní další analytický krok, kterým je seskupení všech úryvků se stejným významem. Dále je možné vzniklé kódy kategorizovat. Jedná se o činnost, ve které výzkumník seskupuje kódy podle jejich podobnosti či jiného kritéria.

Vyšší úroveň analýzy dat představuje **axiální kódování**, které systematicky navazuje na otevřené kódování. Jeho cílem je podle Strausse a Corbinové (1999, s. 71) vytvoření vazeb mezi kategoriemi. Za tímto účelem byl podle Hendla (2016, s. 252) vytvořen **paradigmatický model**, který umožňuje o datech systematicky přemýšlet, ale především k sobě složitějšími postupy vztahovat kategorie vzniklé otevřeným kódováním. Výzkumník prostřednictvím paradigmatického modelu hledá, které kategorie spolu souvisejí. Detailní popis prvků tohoto modelu je možné najít v následující tabulce. Při axiálním kódování výzkumník hledá vazby mezi kategoriemi a uspořádává je do nového schématu. Uvažuje o příčinách a důsledcích, podmínkách a interakcích, strategiích a procesech a propojuje jednotlivé kategorie.

Tabulka 1:Prvky paradigmatického modelu (Hendl, 2016)

Prvek	**Popis**
Příčina	Události, případy a procesy, které vedou k výskytu, vzniku, vývoji nebo změnám nějakého jevu. Jedná se o příčiny a jejich vlastnosti.
Fenomén	Ústřední myšlenka, událost, případ či proces, se kterým mají interakce a jednání nějaký vztah. Jev drží celý paradigmatický model pohromadě. Obvykle to je to ústřední téma výzkumu.
Kontext	Konkrétní soubor vlastností, které jevu náleží. Jde o soubor konkrétních podmínek, za nichž jsou uplatňovány strategie jednání nebo interakce.
Intervenující podmínky	Podmínky související se strategiemi jednání nebo interakce, které jevu náleží.
Strategie jednání	Cílené a záměrné aktivity, které jsou odpovědí na jev a intervenující podmínky.
Následky	Výsledky či důsledky jednání a interakce.

Posledním krokem je **selektivní kódování**, jímž začíná integrace výsledků v zakotvené teorii. Podkladem jsou výsledky z axiálního kódování a cílem je vyhledání hlavního

tématu a sjednocení témat, které výzkumník předchozími analytickými kroky ve svých datech identifikoval. Ústředním pojmem selektivního kódování je dle Strausse a Corbinové (1999, s. 86–88) centrální kategorie, kolem které se organizuje základní analytický příběh. Centrální kategorie by měla odpovídat zkoumanému jevu a dobře jej popisovat. Obvykle jde o tu kategorii, která je do paradigmatického modelu u axiálního kódování zasazena jako fenomén. K centrální kategorii jsou potom vztaženy ostatní kategorie. Selektivní kódování vyžaduje vyšší stupeň abstrakce.

Obrázek 7: Základ axiálního kódování (Hendl, 2016)

Výsledkem všech kroků, tedy otevřeného, axiálního a selektivního kódování je nová teorie, která je zakotvena v datech. Teorie vzniklá z výzkumu je tak z velké části závislá na vedení výzkumu, práci s daty i zkušenostech.

Zpráva o výzkumu pomocí zakotvené teorie lze podle Hendla (2016, s. 349) prezentovat dvěma způsoby. První je rekonstrukce případu, u které autor neuvádí celou historii případu, ale spíše se zaměřuje na abstrakci a formulaci teorie. Druhý způsob přestavuje detailní popis případu, na který je aplikována teorie.

Metody otevřeného a axiálního kódování byly v dizertační práci použity pro zpracování dat a vyhodnocení výsledků hloubkových rozhovorů. V práci byl také zpracován paradigmatický model. Otevřené kódování, zaměřené na pečlivé studium údajů, bylo využito u analýzy hloubkových rozhovorů. Na základě kódů byly sestaveny kategorie a definovány vztahy mezi nimi. Pomocí axiální kódování byly analyzované údaje znovu uspořádány za účelem vytvoření logických spojení mezi kategoriemi. Tímto kódováním byly identifikovány prvky, které tvoří kontext problematiky identifikace nedostatků v rámci hodnocení informačních systémů.

2.3.2 Analýza dat případové studie

Analýza dat případové studie není dle Hendla (2016, s. 229–230, 346) pevně spjata se specifickým přístupem, obecně ji však lze uchopit **holisticky** nebo **analyticky**. Holistická analýza hledá závěry posouzením dat jako celku, naproti tomu analytický způsob je více systematický a je možné ho dále rozlišovat dle typu na analýzu orientovanou na proměnné a analýzu orientovanou na případ. Analýza orientovaná na proměnné se zabývá vztahy mezi koncepty. Analýza orientovaná na případ, která bude využita v rámci dizertační práce, je zaměřená na proces a hledá příčiny a následky uvnitř případu.

Analýza dat případové studie trvá tak dlouho, než se podaří zodpovědět výzkumné otázky. Technikám, které usnadňují tuto analýzu, je věnován tento odstavec. Prvním krokem je sběr dat, jejich uchování a organizace. Jedná se především o transkripci získaných dat do lépe zpracovatelné podoby. Poté následuje segmentace dat, jejímž cílem je rozdělení dat do analytických adresářů, a kódování, které pomáhá data lépe popsat (viz kapitola 2.3.1). Poznámkování přispívá při analýze dat případové studie zachytit zmínky o kódech a jejich vztazích. K dalším technikám se řadí identifikace vztahů mezi kategoriemi a zobrazení pomocí přehledových tabulek a grafů. Průběžný souhrn slouží k popisu toho, co se odhalilo a co je nutné dále analyzovat. Tyto souhrny se postupně iterují do podoby závěrečné zprávy. Mezi další techniky patří použití miniatur, které představují cílený popis série událostí, jež je reprezentativní pro určitý aspekt případu. Všechny popsané techniky byly využity ve fázi ověření metodiky v praxi.

Pro ověření metodiky hodnocení informačních systémů v praxi byla v této práci použita mnohonásobná případová studie. Analýza dat mnohonásobné případové studie je podobná analýze jednoho případu, rozdíl je ale v organizaci dat. Každý případ se nejdříve analyzuje zvlášť a poté dochází ke srovnání všech případů mezi sebou. Je možné využít tabulku obsahující zjištěné jevy pro jednotlivé případy. Na tomto základě poté může dojít ke třízení a abstrakci. Jako pomocnou metodu lze použít analytickou indukci. Ta vychází z předpokladu, že výzkumník má formulovat tvrzení, které platí pro všechny případy.

Při návrhu struktury výzkumné zprávy případové studie je možné uplatnit následujících pět schémat: narativní struktura, komparativní struktura, chronologická struktura, inverzní struktura a struktura navrhování teorie. V této práci byla použita komparativní struktura, která obsahuje části, které postupně rozebírají jednotlivé případy.

2.3.3 Statistická analýza

Statistický přístup ke zkoumání reality vychází podle Součka (2006, s. 5) z potřeby získání základních číselných charakteristik statistického souboru. Na tomto základě je možné v přehledné podobě jednoznačně specifikovat vlastnosti hodnoceného souboru.

Zkoumání hromadných jevů předpokládá dle Budíkové (2010, s. 13–19) definování vymezené množiny objektů zkoumání neboli statistického souboru a jeho prvků, které jsou nositeli vlastností daného souboru. Počet jednotek statistického souboru se nazývá rozsah souboru. Soubory, které jsou předmětem zkoumání, označujeme jako **základní soubor** (někdy se základní soubor označuje jako populace). Hendl (2015, s. 41–42) dodává, že v praxi často z různých důvodů nepracujeme s celým rozsahem statistického souboru, ale jen se vzorkem statistických jednotek neboli s výběrovým souborem. K tomu dochází buď proto, že zkoumání celého statistického souboru by bylo nákladné, časově zdlouhavé nebo z jiných praktických ohledů neuskutečnitelné, anebo proto, že zobecnění provedené z dat výběrového souboru považujeme pro daný účel zkoumání za dostatečně přesné a z hlediska poznání za reprezentativní.

Výběr prvků provádí výzkumník dle Hendla (2015, s. 50–55) tak, aby vytvořený výběrový soubor co nejlépe reprezentoval základní soubor. Nejlepší výběrový soubor je takový, který je zmenšeninou základního souboru. Obecně platí, že čím je rozsah výběrového souboru větší, tím je větší pravděpodobnost, že bude dobře reprezentovat základní soubor.

Výsledky statistického zjišťování mají obvykle povahu velkého a nepřehledného množství číselných údajů, které je třeba pro analýzu vhodně uspořádat a utřídit. Tříděním rozumíme rozdělení jednotek souboru do skupin tak, aby vynikly charakteristické vlastnosti zkoumaných jevů.

Pro základní deskripci statistického souboru kvantitativního znaku se používá dle Neubauera a kol. (2016, s. 31) **systém popisných charakteristik**, který tvoří: míry úrovně hodnot souboru, míry variability hodnot a míry šikmosti (asymetrie) rozdělení. K nejužívanějším mírám úrovně patří aritmetický průměr, medián a modus.

Statistická analýza byla v dizertační práci využita v procesu vyhodnocování výsledků hloubkových rozhovorů. Výsledkem bylo zjištění nejčastějších nedostatků v oblasti provozu a řízení informačních systémů.

3 SOUČASNÝ STAV VĚDECKÉHO POZNÁNÍ

Kapitola se zaměřuje na zhodnocení současného stavu vědeckého poznání v oblasti hodnocení informačních systémů. Přehled literatury je založen na článcích publikovaných v zahraničních i tuzemských časopisech zveřejněných v databázích Science Direct, Emerald, EBSCO, Scopus a Web of Science. Publikace byly získány v rámci plného přístupu VUT v Brně v letech 2012 až 2017. V práci jsou také zahrnuty normy, standardy a odborné publikace českých i zahraničních autorů, kteří se danou problematikou zabývají.

Celkem se v této práci objevuje **126 odkazů na odbornou literaturu**. V případě odborných článku bylo z přibližného počtu 3 500 publikací provedeno časové omezení, dále byla stanovena podmínka na úplnost článku a jeho zaměření do oblasti této dizertační práce. Celkem tak bylo zpracováno 46 odborných článků a vysokoškolských prací za posledních 25 let. Zbývající odkazy se vážou na odborné publikace a standardy.

Cílem kapitoly je vytvořit ucelený přehled relevantních a aktuálních publikací v oblasti hodnocení informačních systémů. V první podkapitole (3.1) jsou vymezeny základní pojmy vztahující se k tématu výzkumu, druhá podkapitola (3.2) se věnuje popisu současného stavu standardů v oblasti posouzení a řízení IS/ICT a třetí podkapitola (3.3) se zabývá popisem současného stavu vědeckého poznání. Poslední podkapitola (3.4) uvádí závěry z celého průzkumu a sumarizuje údaje z literatury a praxe na zkoumané téma.

3.1 Vymezení základních pojmů

V této kapitole je uvedeno několik pojmů, které se bezprostředně vztahují k tématu práce a jejich vysvětlení je chápáno jako první krok k porozumění problematice dizertační práce. Nejdříve jsou zde definovány základní pojmy jako informace, systém nebo systémová integrace, jejichž popis vrcholí vysvětlením informačního systému a souvisejících pojmů (kap. 3.1.1). Následně navazují podkapitoly obsahující pojmy, které se vztahují k řízení, bezpečnosti a auditu informačních systémů (kap. 3.1.2). Jedná se především o strategii, vizi a misi podniku v oblasti informačních systémů, správu systému v dodavatelsko-odběratelských vztazích, efektivnost informačních systémů, řízení výdajů a identifikace přínosů v oblasti IS/ICT, kritéria pro hodnocení investic a integrovaný systém řízení IMS. Kapitola zabývající se auditem (kap. 3.1.3) poté popisuje různé standardy, které lze přímo i nepřímo využit pro hodnocení informačních systémů.

3.1.1 Systémové vymezení informačních systémů

Informace definuje Truneček (2004, s. 13) jako účelově zpracovaná data, kterým jejich uživatel v procesu interpretace přiřazuje určitý význam. **Data** představují vše, co můžeme vnímat našimi smysly a lze je chápat jako surovinu pro vytváření informací. Mládková (2005, s. 6–7) ještě doplňuje, že informace mají nehmotný charakter a vznikají porozuměním a interpretací dat. Na základě informací se v lidské mysli vytváří znalost, která svému majiteli přináší určitou hodnotu.

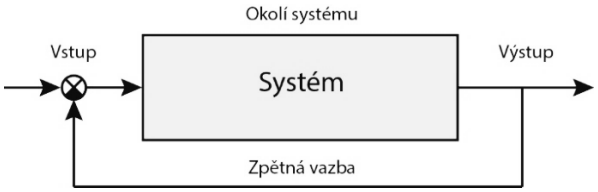
Systém definuje Dostál (2008, s. 6) jako účelově uspořádanou množinu prvků a vazeb mezi nimi. V rámci dekompozice systému lze vyčlenit podsystém, který představuje podmnožinu systémových prvků a vazeb, které je vyčleněny ze systému a jsou chápány jako nový systém nebo prvek. Prvek je dle Janíčka a Marka (2013, s. 40) část systému, který tvoří na dané rozlišovací úrovni dále nedělitelný celek, jehož strukturu nechceme nebo již nemůžeme rozlišit. Rozlišovací úrovní se označuje stupeň podrobnosti zkoumání systému. Dekompozicí systému na jednodušší prvky se zvyšuje rozlišovací úroveň.

Systémová integrace je podle Svozilové (2016, s. 49) kombinací systémů a jejich částí do jednotlivého a funkčního technologického celku při zachování všech procesních potřeb uživatele nebo skupiny uživatelů systému. Systémová integrace představuje jeden ze stěžejních bodů v řešení efektivity vynakládání prostředků. Janíček (2007, s. 60) doplňuje, že v praxi pak poskytuje nástroje pro údržbu systému na všech úrovních řízení. Její možnosti jsou široké, sahají od integrace vizí společnosti přes integraci vnějších a vnitřních procesů až po integraci technologickou, funkční a metodickou.

Informační systém lze dle Tvrdíkové (2008, s. 18) definovat jako soubor lidí, metod a technických prostředků zajišťující sběr, přenos, uchování, zpracování a prezentaci dat. Podobnou definici předkládá i Gála (2015, s. 20–23), který definuje informační systém uspořádání vztahů mezi lidmi, datovými a informačními zdroji a procedurami jejich zpracování za účelem dosažení stanovených cílů. Informační systém je přizpůsobený pro práci s daty, ze kterých se stávají informace a jejich zpracováním a využitím vzniká užitek. Z výše zmíněného je patrné, že informace vznikají z dat a jen příjemce rozhoduje, jak se získanou informací naloží.

Podle Druckera (1993, s. 26) jsou informace jediným smysluplným zdrojem pro podnikání, ostatní výrobní faktory se stávají druhořadými. Díky výše zmíněnému výroku se lze na problematiku dívat i z jiného úhlu pohledu a informace tak lze povýšit k základním výrobním faktorům podnikání. Informační revoluce, o které se mluví v souvislosti s rozvojem informačních technologií, nemusí spočívat v rychlosti zpracování dat, ale ve změně koncepce, kde nositeli revoluce nemusí být technologie, ale samotní lidé. Tento koncept kladně koreluje se vznikem znalostní společnosti, a jak dodává Švarcová a Rain (2011, s. 84–85), s důrazem na řízení znalostí a navazuje na trend učící se organizace.

Informační systém lze popsat jako **kybernetický systém**, tedy sociálně technický systém, který se dělí dle Janíčka (2007, s. 7) na řídící, např. zaměstnanec firmy, a řízený, např. technické zařízení. Důležitá je v tomto případě zpětná vazba, jež uskutečňuje cílové chování celého systému, které může představovat tvorbu hodnoty pro vlastníky.



Obrázek 8: Systémové vymezení problému (Janíček, 2007)

Klíčovým zdrojem metodiky navržené v rámci dizertační práce je tvorba modelu, na jehož základě je možné posoudit nezbytné charakteristiky informačního systému. Na základě simulace s využitím reálných vstupů a výstupů bude možné navrhnout změny. Z pohledu této dizertační práce lze informační systém firmy dekomponovat na podsystémy, které obsahují moduly informačního systému, tedy jednotlivé komponenty, které na dané rozlišovací úrovni řeší úlohy nezbytné pro chod společnosti. Blízké okolí takto nastíněného systému představují samotní uživatelé, tedy zaměstnanci firmy. Dodavatelské a odběratelské vztahy pak definují okolí vzdálené. Vstup systému je definován jako vstupní informace od zákazníka, např. poptávka. Spolu s dílčími vstupy čítající např. zásoby a materiál se úvodní informace transformuje na výstup, jenž může v daném okamžiku představovat požadovaný produkt či službu.

3.1.2 Řízení informačních systémů

Strategické řízení zahrnuje dle Smejkala a Raise (2013, s. 40–43) činnosti zaměřené na dlouhodobý soulad mezi vizí firmy, jejími cíli a disponibilními zdroji. Každá společnost existuje proto, aby naplňovala určité poslání. Toto poslání je zakotveno v **misi** společnosti a koresponduje s **vizí** společnosti, která obsahuje představu zakladatelů firmy o tom, co bude předmětem podnikání, jací budou zákazníci firmy, jaké potřeby a jakými výrobky a službami bude firma potřeby svých zákazníků uspokojovat. Dohnal a Příklenk (2011, s. 58–59) dodávají, že vize a mise má velký význam hlavně proto, aby všichni ve firmě směřovali stejným směrem.

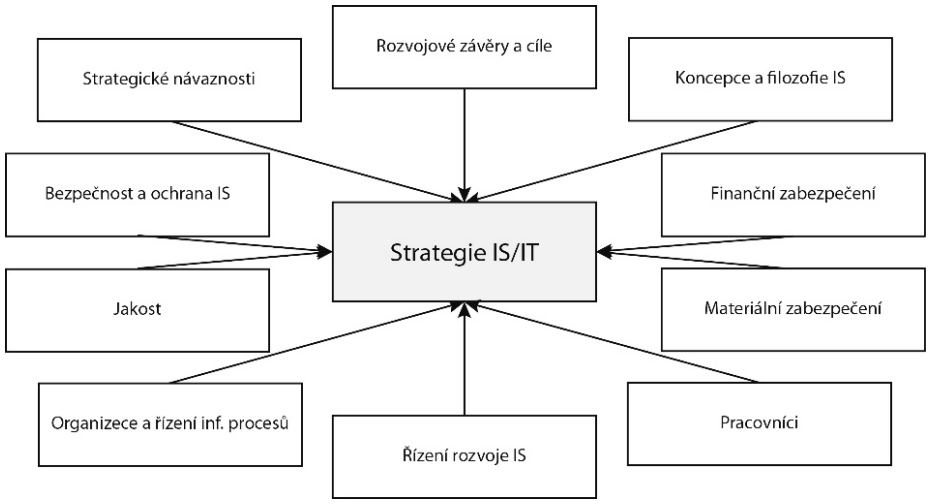
Strategie ukazuje základní představy o tom, jakou cestou budou firemní cíle dosaženy. Tyto strategie lze dle Keřkovského a Vykypěla (2006, s. 25–38) rozlišit na firemní, obchodní a funkční. Firemní strategie (*Corporate strategy*) představuje základní podnikatelské rozhodnutí o odvětví a zdrojích podnikání. Na firemní strategii navazuje obchodní strategie (*Business strategy*), která je rozpracována pro každou strategickou obchodní jednotku SBU (*Strategic Business Unit*) vymezenou na základě zákazníků a jejich potřeb. Hierarchicky nejníže figurují funkční strategie, které se věnují specifickým oblastem firmy, jako jsou například marketing, výzkum a vývoj nebo podniková informatika.

Strategie úzce souvisí s firemními cíli, o kterých lze obecně říci, že představují žádoucí stavy, kterých má být dosaženo. Cíle by měly být jasně zadány, a proto je výhodné pro jejich definování použít metodu **SMART**. Cíle sestavené podle této techniky by měly být dle Červeného a kol. (2014, s. 16) specifické a jasné (*Specific*), měřitelné (*Measurable*), dosažitelné (*Achievable*), relevantní (*Relevant*) a časově vyhraněné (*Time-bound*).

Dle **organizační hierarchie** je možné v podniku identifikovat úrovně strategického, taktického a operativního řízení. Každá z těchto rovin vyžaduje specifický způsob zpracování nebo druh informací. Svou roli zde hraje podle Keřkovského a Vykypěla (2006, s. 4–5) časový horizont, podrobnost, zdroje, stupeň určitosti a frekvence výskytu. Zmíněné faktory společně s hierarchií strategických plánů představují jedno z východisek pro strategické řízení informačních systémů a zdůrazňují různou potřebu informací ve vztahu k metodám jejich získání.

S vývojem informačních technologií vzrostlo povědomí o strategickém významu informací. Současně se také přizpůsobovala pozice informatiky v organizační struktuře společností a cíle řízení informačních systémů. Tento vývoj vedl k definování informační strategie, která má představu o tom, jak budou cíle spojené s IS/ICT dosaženy. Dle Sodomky a Klčové (2010, s. 53–54) lze strategické řízení IS/ICT definovat jako kontinuální proces, jehož cílem je efektivně využít informačních systémů a technologií k vytváření přidané hodnoty produktů a služeb, které organizace nabízí zákazníkům.

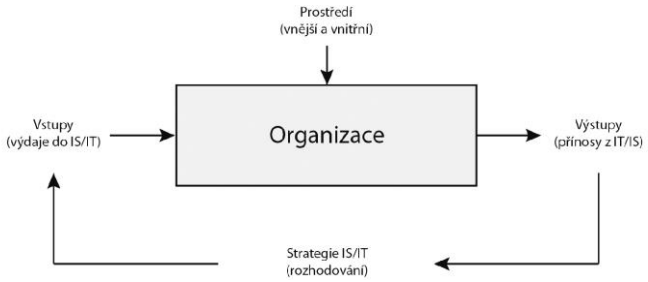
Podle Keřkovského (2015, s. 22) vytyčuje informační strategie strategické cíle a cesty jejich realizace ve vztahu k podnikovým informačním systémům a technologiím. Dle strategického řízení firmy je definována jako funkční strategie, která je pevně svázána s ostatními funkčními strategiemi, a proto by tvorba strategických cílů spojených s IS/ICT měla zohledňovat ostatní cíle podniku. Možné obsahové řešení informační strategie dle Červeného a kol. (2014, s. 37) je znázorněno na obrázku č. 9.



Obrázek 9: Obsahové vymezení informační strategie (Červený a kol., 2014)

Boddy a kol. (2008, s. 102–108) shrnuje realizaci informační strategie do několika základních bodů. První krok představuje provedení analýzy současného stavu a na tomto základu se definují strategické cíle. Poté následuje zpracování plánu pro jejich dosažení, který by měl splňovat podmínky variantnosti a permanentnosti. Po vyhodnocení a výběru strategie přichází na řadu její implementace a kontrola.

Strategické plány informační strategie se zabývají popisem přínosů, výdajů a finančním ohodnocením projektů, které se vztahují k podnikové informatice. Strategie může být také doplněna o charakteristiky aplikačních, funkčních, datových a technologických architektur, které se zabývají možností integrace všech zmíněných aspektů. Pro zajištění rozvoje je dobré strategii ještě rozšířit o nejvhodnější technologickou infrastrukturu skládající se z hardwaru, softwaru a komunikačních technologií. Ze syntézy všech zmíněných poznatků vyplývá, že informační strategie má hlavní postavení v řešení efektivnosti informačních systémů, tak jak je vidět na níže uvedeném obrázku č. 10.



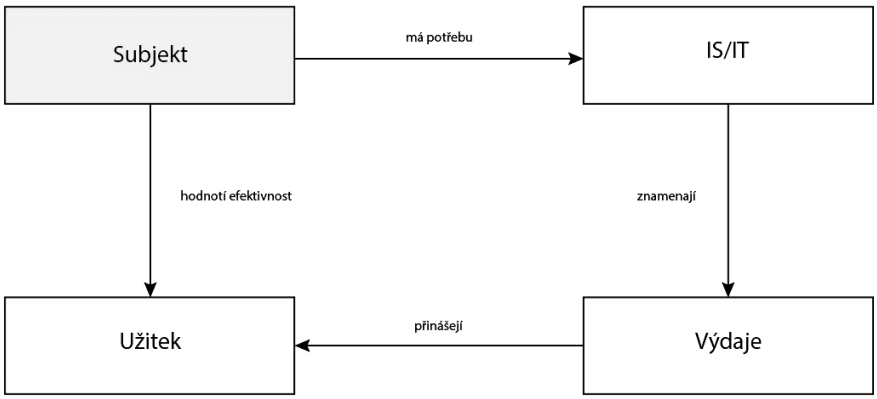
Obrázek 10: Koncepční schéma modelu efektivnosti (Molnár a kol., 1999)

Řízení informatiky lze dle Doucka a kol. (2008, s. 40–48) či Gály (2015, s. 39) dělit na dvě koncepce: **IT Governance** a **IT Servise Management**. IT Governance zahrnuje širší pojetí, které jde ruku v ruce se strategickými hledisky organizace. Cílem je definovat strategické cíle informatiky v souladu s potřebami a zájmy organizace jako celku. Cílem Corporate Governance je dle Ministerstva financí České republiky (2004) formulovat a rozvíjet právní a výkonné metody a postupy, které zavazují společnosti udržovat vyvážený vztah mezi organizacemi a všemi zainteresovanými stranami. Enterprise Governance je problematika strategického řízení organizace. Cílem Business Governance jsou nízké náklady, konkurenceschopnost a zisk organizace. IT Servise Management představuje řízení služeb IS/ICT na operativní úrovni. Cílem je účelně a účinně realizovat cíle stanovené řízením informatiky. Inspiraci lze hledat v „Best practise“, které představují jakousi šablonu či standard v nastavování procesů v organizacích. Lze používat doporučení poradenských firem, zkušených manažerů nebo doporučení, která jsou popsaná v nějakém standardu či frameworku.

S řízením informačních systémů se také zavádí správa systému v dodavatelsko-odběratelských vztazích, označovaná jako **SLM** *(Service Level Management),* kterou

popisuje ve své publikaci například Lukáč (2011, s. 147–153). Jedná se o proces, který definuje služby, které souvisí s poskytováním, strukturou a měřením IS/ICT. Na základě přání zákazníka, který své požadavky definuje v požadavcích na úroveň služby **SLR** *(Service Level Requirement)*, vzniká dohoda o úrovni služby **SLA** *(Service Level Agreement)*. SLA definuje dle Učně (2001, s. 40) rozsah infrastruktury, popis všech činností služby, spolehlivost služby, dostupnost služby, bezpečnost i záložní plány.

Efektivnost informačních systémů je možné popsat podle Molnára (2000, s. 16) jako transformaci vstupů na výstupy s podmínkou vnějších a vnitřních faktorů. Vstup je charakterizován výdaji do IS/ICT a výstup přínosy IS/ICT, podle kterých se následně hodnotí účinnost. Na základě informační strategie, která je spojena s rozhodováním, se pak stanovuje takové složení a velikost vstupů, aby výstup, tedy přínos, byl co nejvyšší. V řízení efektivnosti informačních systémů jde tedy o sledování výdajů a přínosů. Hodnocení efektivnosti se nezabývá pouze uspokojováním potřeb, ale také očekáváním uživatelů. Každý z nich má ovšem jiné požadavky na podnikové informační systémy a dle nich lze identifikovat čtyři skupiny: majitele, manažery zaměstnance a zákazníky. Majitelé očekávají trvalé zhodnocení majetku, manažeři vyšší podporu řízení, zaměstnanci lepší pracovní prostředí a zákazníci kvalitnější produkty a služby.



Obrázek 11: Model užitku (Molnár, 2000)

Řízení výdajů představuje podle Molnára (2000, s. 27) hledání maximálního užitku při daných finančních prostředcích, nebo pevně daném užitku a hledání cesty, jak ušetřit co nejvíce finančních prostředků. Výdajovou stránku ale nelze posuzovat jen z pohledu velikosti vynaložených finančních prostředků, protože zde není přímá souvislost mezi

velikostí výdajů a přínosů. Neplatí tedy, že čím více bude utraceno, tím více bude přínosů. Dle ekonomické teorie lze u výdajů definovat stav nasycení, kdy již další výdaje nezvyšují přínosy. Závislost je poté nutné hledat v dalších faktorech, jedním z nich je účelnost výdajů. Výdaje na IS/ICT je potřeba sledovat v poměrových číslech ve vztahu k historii a velikosti podniku, aby bylo možné mezipodnikové srovnání a analýza trendu. Výdaje na IS/ICT lze rozdělit podle času, druhu a aplikací. Sledování výdajů je stěžejním bodem pro plánování a controlling.

Přínosy ze zavedení informačních systémů a technologií lze dát dle autorů Irani a Love (2008, s. 18–19) obecně do souvislosti se strategickým plánováním. Na základě strategických plánů je totiž možné identifikovat a hodnotit přínosy dle různých kritérií. Cílem by však měl vždy být spokojený uživatel, jako hlavní hybná síla efektivnosti podnikového informačního systému. Proto by se právě uživateli měla věnovat velká pozornost.

Přínosy ze zavedení IS/ICT rozděluje Molnár (2000, s 49) podle následujících hledisek:

- finanční a nefinanční přínosy (měřitelné v jiných než finančních jednotkách),
- kvantitativní (měřitelné dle stupnice) a kvalitativní (dle logické hodnoty),
- přímé (přímý vztah k přínosu) a nepřímé,
- krátkodobé a dlouhodobé,
- absolutní a relativní.

Pomocí výše uvedených ukazatelů je možné hodnotit účelnost, poměr mezi dosaženou a plánovanou hodnotou. Proto je důležité umět tyto přínosy odhadnout a následně vyhodnotit. Příkladem přímých ekonomických přínosů může být například zkrácení doby výroby nebo úspora pracovních sil. Nepřímým přínosem může být zvýšení konkurenceschopnosti podniku.

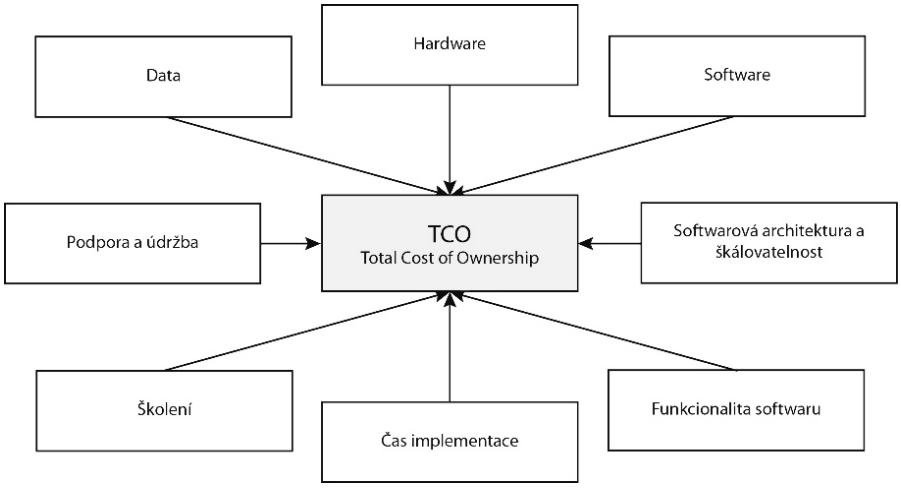
Na základě plánu rozvoje informačních systémů a technologií je třeba rozhodnout, zda je výhodné do daného projektu investovat. Obecně je dle Vochozky a Mulače (2012, s. 270–286) proces svázán s kvantifikací příjmů a výdajů z investice a rozhodnutím, jestli je ekonomicky výhodné požadovaný projekt realizovat. Irani a Love (2008, s. 20–21) definují mnoho kritérií pro hodnocení investic, které lze jednoduše rozdělit na kritéria finančního a nefinančního charakteru. Tímto je definována důležitost vztahu mezi informační strategií a finančním ohodnocením investice. Pro finanční hodnocení

efektivnosti investičních projektů je nejdůležitější kapitálové plánování, které je zahrnuto v dlouhodobém finančním plánu investiční činnosti. Jedná se o rozhodování v delších časových horizontech, počítá se s většími odchylkami i s časovou i kapitálovou náročností. Stěžejní částí je rozhodovací proces, který detailně posuzuje danou investici. Jeho východiskem je posouzení investiční činnosti, kde je důležité kvantifikovat všechny kapitálové příjmy a výdaje, které souvisí s investičním záměrem. Důležité položky byly shrnuty v předcházejících kapitolách. Do kapitálových výdajů se řadí veškeré vynaložené výdaje na investici, které představují například výdaje na pořízení nové investice nebo trvalý přírůstek oběžného majetku. Následně přichází na řadu stanovení očekávaných toků z investice, které představují roční příjmy během doby životnosti.

Po dokončení investičního plánu je možné přikročit k finančnímu hodnocení investice, jehož metody jsou nastaveny na maximalizaci tržní hodnoty podniku. K nejdůležitějším patří dle Režňákové (2005, s. 53–55) **čistá současná hodnota** *(Net Present Value)*, která představuje rozdíl mezi diskontovanými peněžními příjmy z investice a kapitálovými výdaji, kdy je pro podnik investice přijatelná pouze v případě, že je ukazatel čisté současné hodnoty větší než nula. Znamená to, že se zvyšuje hodnota podniku. **Index rentability** *(Profitability Index)* představuje poměr diskontovaných peněžních příjmů z investice a kapitálových výdajů. Pro přijmutí investice je nutné, aby byl index vyšší než jedna. **Vnitřní výnosové procento** *(Internal Rate of Return)* je výnosová míra vyjádřená v procentech. Za přijatelnou investici se považuje taková, jejíž výnos je vyšší, než je požadovaná minimální výnosnost investice. **Doba návratnosti** vyjadřuje počet let, za které se výdaje na investici splatí ziskem po zdanění.

Na základě prostředků známých z finanční analýzy je možné použít pro hodnocení poměrové ukazatele **rentability**. Jedná se dle Fotra a Součka (2005, s. 64) o ukazatele rentability vlastního kapitálu ROE *(Return on Equity)*, celkových aktiv ROA *(Return on Assets)* a vloženého kapitálu ROI *(Return on Investments)*. V uvedených ukazatelích se ve spojitosti s IS/ICT sleduje, aby rentabilita s jejich přispěním rostla. Spíše než celkové hodnoty jsou v tomto případě zajímavé rozklady a posléze identifikace položek, které jsou ovlivnitelné pomocí IS/ICT a přispívají k celkové výši indexu. Rozklad může být realizován například pomocí DuPontova diagramu s využitím logaritmické metody.

Dalším finančním ukazatelem, který uvádí například Koch (2010, s. 143–144), je **TCO** *(Total Cost of Ownership)*, jehož výsledkem jsou celkové náklady na implementaci a provoz IS/ICT systémů. Vytvořila jej společnost Gartner (2014), která TCO rozčlenila do čtyř základních kategorií na investice, technickou podporu, řízení a činnosti koncových uživatelů. Ukazatel ale nemusí být použit na již vlastněné prostředky, ale i na plánované investice a může sloužit jako podklad pro rozhodování mezi investičními projekty. Mezi jeho nevýhody patří nadměrné zaměření na náklady spojené s IS/ICT bez zřetele na výnosy. Proto vznikl alternativní koncept **TVO** *(Total Value of Ownership)*, který bere v úvahu dle Vymětala (2009, s. 19) nejen vlastní náklady, ale i přínosy v oblastech IS/ICT. Celkové náklady na vlastnictví tak zahrnují všechny náklady vynaložené v průběhu celého životního cyklu provozovaného systému.



Obrázek 12: Složení ukazatele Total Cost of Ownership (Molnár, 2000)

Drobný problém může nastat v případě, když nelze jednoznačně identifikovat finanční příjmy z dané investice. Pokud tento případ nastane, přichází na řadu převod těchto nefinančních ukazatelů na finanční. Proces probíhá v několika krocích, ve kterých je nutné si uvědomit význam a rozsah každé změny. Výsledek pak představuje odhad finančního ohodnocení.

V souvislosti s finančním plánováním a řízením projektů v oblasti informačních systémů je možné zmínit **integrovaný systém řízení IMS** *(Integrated Management System)*, který se na vedení organizace dívá z následující perspektivy. Jedná se o účinný a efektivní nástroj pro řízení organizace, jehož hlavním rysem je ta vlastnost, že při řízení všech jeho

komponent lze postupovat podle podobných postupů, které jsou zahrnuty v životním cyklu **PDCA**. Zmíněný cyklus se dle Učně (2001, s. 15) skládá se z etap Plánuj *(Plan)*, Dělej *(Do)*, Kontroluj *(Check)* a Jednej *(Act)*. Za komponenty IMS jsou dle Doucka a kol. (2008, s. 20–23) považovány systémy řízení jakosti, vztahu s okolím a bezpečnosti a ochrany zdraví při práci. Pro řízení jakosti **QMS** *(Quality Management System)* je definována norma ISO 9000. Systém řízení procesů zaměřený na vztah organizace k životnímu prostředí **EMS** *(Environmental Management System)* uplatňuje standard ISO 14000. V oblasti bezpečnosti a ochrany zdraví při práci se používá program, který vychází z dokumentu OHSAS 18001. Podobné principy je možné použít i při řízení informatiky.

Ruku v ruce s řešením koncepce řízení IS/ICT je nezbytné definovat několik pojmů z oblasti **řízení rizik**, které zavádí autoři Smejkal a Rais (2013, s 95–101) nebo Gála a kol. (2015, s. 214–217). Aktivum *(Asset)* představuje cokoli v organizaci, co má nějakou cenu, která může být zmenšena působením nějaké hrozby. Základní charakteristikou aktiva je jeho hodnota. Ta může být založena na objektivním vyjádřením ceny (např. pořizovací náklady), subjektivním oceněním důležitosti nebo na kombinaci obou přístupů. Zranitelnost *(Vulnerability)* je slabé místo aktiva. Úroveň zranitelnosti se hodnotí podle dvou faktorů: citlivosti (náchylnost aktiva být poškozeno hrozbou) a kritičnosti (důležitost aktiva pro analyzovaný subjekt). Hrozba *(Treat)* je událost ohrožující bezpečnost (zneužití zranitelnosti). Útok se označuje termínem bezpečnostní incident *(Security incident)*, což představuje jakoukoli událost, která vede k porušení definovaných pravidel nebo pokusů o tato porušení. Riziko *(Risk)* je kombinace hrozby a zranitelnosti s dopadem na aktivum. Zbytkové riziko, je tak malé, že je pro subjekt přijatelné a není nutné podnikat další opatření. Protiopatření *(Countermeasure)* úroveň rizika snižuje. Z pohledu analýzy rizik lze protiopatření charakterizovat efektivitou (nakolik opatření sníží účinek hrozby) a náklady (náklady na pořízení, zavedení a provozování protiopatření). Dopad *(Impact)* představuje vznik škody v důsledku působení hrozby.

3.1.3 Audit informačních systémů

Audit je dle Dvořáčka (2005, s. 2) komplexní formalizované nezávislé prověření kontrol vzhledem k existujícím standardům. Audit interní je dle Kafky (2009, s. 14) prováděný organizační jednotkou firmy a audit prováděný externí organizační jednotkou je označován jako audit externí. Základem všech auditů je finanční neboli statutární audit. Podle Svaté (2011, s. 16) se jedná o proces objektivního získávání a vyhodnocování důkazů, týkajících se informací o ekonomických činnostech a událostech, s cílem zjistit míru souladu mezi těmito informacemi a stanovenými kritérii a sdělit výsledky zainteresovaným zájemcům.

Audit informačních systémů je na mezinárodní úrovni zaštítěn především institucemi ISACA, INTOSAI, SIM, IIA, AITP či ACCA. Na oblast auditu, řízení, kontroly a bezpečnosti informačních systémů se především specializuje instituce **ISACA** *(Information System Audit and Control Association)*, která zastřešuje dle ISACA (2017) vzdělávání v následujících oblastech: CISA *(Certified Information Systems Auditor)*, CISM *(Certified Information Security Manager)*, CGEIT *(Certified in the Governance of Enterprise IT)* a *CRISC (Certified in Risk and Information Systems Control)*.

Problémem, který postihuje audit informačních systémů, je komplexní a dynamický vývoj IS/ICT. Informační technologie a informační systémy se vyvíjí stále rychleji, a proto je velmi důležité neustálé vzdělávání. Jako další úskalí uvádí Svatá (2011, s. 21) způsob dekompozice, míru detailu, časový aspekt a použitou metodiku. V mnoha případech není možné provést audit celého objektu najednou, ale je potřeba zvolit vhodný způsob dekompozice a audit provést postupně. Dekompozice lze provést např. na základě funkce (zpracování mezd), prvku (servery), procesu (změnové řízení) nebo služby (elektronická pošta). Míra detailu určuje, jak podrobně se bude vymezený objekt auditovat (celkový softwarový audit, audit operačního systému, audit aplikace, audit databázového systému). Časový aspekt se týká jak délky samotného auditu, tak doby, za kterou je objekt hodnocen. Dále je potřeba vzít v potaz životní cyklus hodnoceného objektu (audit implementace, audit migrace, audit provozu). Poslední problém představují samotné standardy pro hodnocení IS/ICT. Pro oblast auditu informačních systémů existuje mnoho metodik, rámců, standardů či „Best practise“. Tyto návody mají různé cíle a jsou zpracovány na různé podrobnosti. Detailně se jimi zabývá kapitola 3.2.

3.2 Současný stav standardů v oblasti posouzení a řízení IS/ICT

Mezi nejznámější standardy, normy, procesní rámce a metodiky posouzení a řízení IS/ICT patří dle organizace ISACA (2011) zejména COBIT, ITIL, ISO 9000 a ISO 27000. Kromě těchto hlavních standardů se používají i méně známé, často více specializované, jako například Val IT, Risk IT, INTOSAI nebo PRINCE2. Některé dnes používané normy či standardy jako Sarbanes-Oxley (SOX), Six Sigma, COSO, Balanced Scorecard a další určené pro řízení a měření výkonnosti nebo rizik organizace nebyly původně určeny přímo pro oblast řízení informačních systémů. Situace se nicméně změnila díky dnešní provázanosti informatiky s celým podnikem.

Svatá (2011, s. 170) uvádí ve své publikaci příklady standardů, které zastřešuje IT Governance v čele se standardy COSO, COBIT a SOX. Příslušné grafické zobrazení je možné nalézt na obrázku č. 13. IT Governance pokrývá oblasti od řízení projektů (PMNOK a PRINCE2) přes řízení IT služeb (ITIL), vývoj aplikací (CMMI, ISO 15504, ISO 12207), řízení bezpečnosti informací (ISO 27000), oblast plánování (BSC) až po řízení kvality (ISO 20000 a Six Sigma).

IT Governance					
Řízení projektů	**Řízení IT služeb**	**Vývoj aplikací**	**Řízení bezpečnosti**	**Plánování**	**Řízení kvality**
PMBOK PRINCE2	ITIL	CMMI ISO 15504 ISO 12207	ISO 27000	BSC	ISO 20000 Six Sigma
COSO, COBIT, SOX					

Obrázek 13: Oblasti řízení IT s příklady známých standardů (Svatá, 2011)

Mezi další faktory vstupující do řízení podnikových IS/ICT se řadí i právní normy. Jak uvádí Jech (2010), v České republice se jedná například zákon o ochraně osobních údajů, zákon o elektronickém podpisu nebo některé paragrafy trestního zákoníku. V mezinárodním prostředí stojí za zmínku například Patriot Act nebo HIPAA.

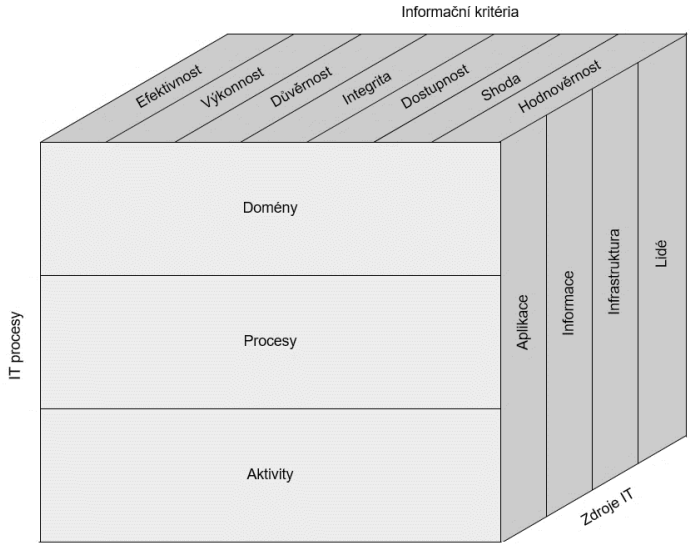
Celkem bylo pro potřeby této práce zahrnuto 25 metodik, standardů či norem. Jejich výčet doplněný o krátký popis je prezentován v tabulce 2. Detailní popis je součástí první podkapitoly, zhodnocení současného stavu pak obsahuje druhá podkapitola.

Tabulka 2:Přehled standardů, norem a postupů používaných v oblasti posouzení a řízeni IS/ICT (Molnár, 2000; Dvořáček, 2005; Doucek a kol., 2008; ISACA, 2011; Svatá, 2011; Pour a kol., 2015)

Standard	Popis
COBIT	Komplexní rámec pro řízení a kontrolu IT.
IT Assurance Guide	Návody na jednotlivé etapy a činnosti životního cyklu auditu.
ITIL	Definuje procesy pro řízení, dodávku a podporu IT služeb.
ISAE	Mezinárodní standardy pro ověření zakázky.
ISA	Mezinárodní auditorské standardy, které se uplatňují při auditu historických účetních informací.
INTOSAI	Doporučení pro audit IS/ICT na základě ISA.
ISO 12207	Definuje procesy určené pro oblasti nákupu, provozu a správy software.
ISO 15504	Definuje procesy určené pro oblasti nákupu, provozu a správy software.
ISO 20000	Norma, která se zaměřuje se na zlepšování kvality, zvyšování efektivity a snížení nákladů u IT procesů.
ISO 27000	Rámec pro zavedení a řízení systému informační bezpečnosti.
ISO 31000	Rámec zaměřený na řízení rizik.
Val IT	Rámec pro řízení investic do IS/ICT a jejich návratnosti.
COSO ERM	Zaměřeno na identifikaci událostí a efektivní řízení rizik.
CRAMM	Metodika zabývající se řízením bezpečnosti a analýzou rizik.
RAMSES	Metodika zabývající se řízením bezpečnosti a analýzou rizik.
OCTAVE	Metodika zabývající se řízením bezpečnosti a analýzou rizik.
Risk IT	Rámec pro řízení rizik aplikovatelný přímo pro oblast IS/ICT.
BSC	Systém měření a řízení výkonnosti organizace.
Six Sigma	Koncept směřující k odstraňování problémů s kvalitou produkce.
PRINCE2	Standard pro projektový management.
PMBOK	Standard pro projektový management.
CMMI	Framework zaměřený na zlepšování procesu vývoje nového produktu.
SOX	Zákon, který zavádí povinnost manažerů a auditorů vyjádřit se k interním kontrolním systémům.
PCAOB	Rada pověřená dohledem nad auditorskou profesí.
BASEL II	Dohoda, jejíž cílem je vytváření podmínek pro stabilní bankovní sektor.

3.2.1 Přehled standardů v oblasti posouzení a řízení IS/ICT

COBIT *(Control Objectives for Information and Related Technologies)* je dnes dle studie ISACA (2011) jedním z nejrozšířenějších standardů v této oblasti posouzení a řízení IS/ICT. Cílem metodiky je pomoci organizacím maximalizovat užitek plynoucí z informačních technologií díky návodům, ukazatelům a popisům nejlepších praktických zkušeností. Základní princip metodiky je dle Gály a kol. (2015, s. 184) postaven na strategických požadavcích organizace, zdrojích a procesech, jejichž vzájemné prolnutí znázorňuje kostka COBIT na obrázku č. 14. ISACA (2012) dále definuje, že základní princip metodiky je postaven na cílech organizace, zdrojích informačních technologií a procesech. Tyto tři komponenty jsou také zobrazeny na kostce COBIT, která přehledně znázorňuje prolínání procesů IT (na úrovni domén, procesu a aktivit), zdrojů informatiky (aplikace, informace, infrastruktura a lidé) a požadavků na informační kritéria (efektivnost, výkonnost, důvěrnost, integrita, dostupnost, shoda, hodnověrnost).



Obrázek 14: Kostka COBIT (Ondrák a kol., 2013)

Příručka od ISACA (2012) dále uvádí, že metodika definuje čtyři domény: plánování a organizace, akvizice a implementace, dodávka a podpora a sledování a hodnocení. Metodikou COBIT se na akademické půdě zabývá mnoho autorů. Z pohledu tématu hodnocení informačních systémů je zajímavá studie autora Panopoulose (2012), která se zabývá implementací metodiky pro účely IS/ICT auditu, nebo autora Suryani a kol. (2015), který popisuje možnosti provedení auditu účetního systému s využitím metodiky COBIT.

ISACA (2007) ještě doplňuje, že kromě základních dokumentů poskytuje metodika COBIT i návody zaměřené na audit informačních systémů, konkrétně **IT Governance Implementation Guide: Using Cobit and Val IT** a **IT Assurance Guide: Using Cobit**. Cílem druhého zmíněného dokumentu je podle Svaté (2011, s. 92) poskytnout návody na jednotlivé etapy a činnosti životního cyklu auditu a ujištění. Auditor pak může poskytnout záruky o dodržování kontrol, hodnotit rizika vyplývající z nedodržování kontrol a doporučit opravná opatření. Vlastní postup hodnocení je popsán pomocí životního cyklu, který se skládá z etapy plánování, stanovení rozsahu a realizace.

Dalším nástrojem z dílny organizace ISACA je rámec **Val IT**, který slouží pro řízení investic a jejich návratnosti do IS/ICT. Cílem je dle ISACA (2008) definovat přidanou hodnotu pro podnik plynoucí z implementace IS/ICT řešení. Val IT je úzce spjat s metodikou COBIT, kterou rozšiřuje a doplňuje z obchodního a finančního hlediska. Thorp (2008) dodává, že klíčovým pojmem je hodnota IS/ICT investice, za kterou se považuje přínos investice po celou dobu životního cyklu. Kromě finanční hodnoty se berou v úvahu i nefinanční přínosy. Metodika je organizovaná do tří domén: správa a řízení hodnot *(Value Governance)*, řízení portfolia *(Portfolio Management)* a řízení investic *(Investment Management)*. Společně s metodikou pro identifikaci rizik použili tento rámec autoři Mushtaque a kol. (2014) pro ohodnocení investic v bankovním sektoru. Aplikací ve veřejném sektoru se zabývá studie autorů Wilkin a kol. (2013).

Doporučené a osvědčené přístupy **ITIL** *(Information Technology Infrastructure Library)* představuje soubor knih popisujících způsoby procesního řízení služeb včetně IT infrastruktury. Bucksteeg (2012, s. 22) dodává, že jejím cílem je poskytnout nejlepší zkušenosti z oblasti informačních technologií. ITIL prochází neustálým vývojem, aktuální je verze 3, která přináší pohled na IT z pohledu životního cyklu služeb. Gála a kol. (2015, s. 183) dále popisuje rozdělení metodiky ITIL do fází obsahující strategii služeb, návrh služeb, přechod služeb, provoz služeb a neustálé zlepšování služeb. ITIL propojuje vlastní procesy s obchodní strategií s důrazem na fakt, že informační strategie musí vycházet z potřeb zákazníků a organizace. Tyto doporučené přístupy představují standard pro řízení služeb v IS/ICT, zlepšování kvality, zvyšování efektivnosti a redukci nákladů. Efektivitou auditu informačních systémů ve firmě, která má zavedený ITIL, se zabývá například studie autorů Wahyudi a Deswadi (2016).

Při správě a vývoji software se lze setkat podle Jecha (2010) s **ISO 12207** a **ISO 15504**. Směrnice je deklarována mezinárodní normou, podle které se posuzuje kvalita procesů vývoje, správy a nákupu softwarů. Celkem je definováno 24 procesů jako např. vývoj, nákup, dokumentace nebo řízení rizik či řízení lidských zdrojů. Pro ohodnocení kvality se používají úrovně, které vyjadřují stupeň vyspělosti procesní oblasti v organizaci.

ISO 20000 je první standard, který se speciálně vztahuje k managementu služeb IS/ICT a zaměřuje se na zlepšování kvality, zvyšování efektivity a snížení nákladů u IS/ICT procesů. ISO 20000, které vzešlo ze standardu BS 15000, popisuje integrovanou sadu procesů řízení pro poskytování služeb IS/ICT a obsahově se řídí ustanoveními ITIL. Sodomka a Klčová (2010, s. 59) dodávají, že norma dále stanovuje požadavky na systém managementu IT služeb. Jedná se především o požadavky na plánování, vytvoření, zavedení, provoz, monitorování, přezkoumání a zlepšování. Přínos implementace normy pro organizace zkoumá například Cots a kol. (2016), který ve své práci oslovil 105 firem a vytvořil model pro zjišťování přínosů implementace.

Pro jakýkoli podnik, který se chce prosadit na dnešním trhu, je nezbytné, aby zpracovával velké množství informací. Tyto informace mohou být pro společnost velmi cenné, a právě proto je potřeba přemýšlet, jak je co nejlépe zabezpečit. Tento fakt je nutným východiskem pro systémové řízení bezpečnosti informací v podniku, ve kterém jde o zabezpečení celého životního cyklu informace od jejího nabytí, po celou dobu zpracovávání, uložení a smazání. Zmíněné postupy, které popisuje ve své publikaci Doucek a kol. (2008, s. 95–96), jsou harmonizovány a integrovány v systému řízení bezpečnosti informací **ISMS** *(Information Security Management System)* a dále podpořeny řadou norem pro řízení informační bezpečnosti **ISO 27000**. S řízením rizik obecně se pojí směrnice **ISO 31000**, která dle ČSN ISO 31000 (2010) poskytuje návody, jak řídit systematickým, transparentním a spolehlivým způsobem různé formy rizik a jak harmonizovat systému řízení rizik do organizace a všech jejích procesů, rozhodování, produktů, služeb a aktiv. Hodnocením informačních systémů ve vztahu k bezpečnostním normám se zabývají ve svých článcích například autoři Duncan a Whittington (2014), kteří zkoumali nesoulad mezi normami bezpečnosti, auditem a skutečnými požadavky na bezpečnost a jejich dopad na společnost, nebo Ryoo a kol. (2014), který se zaměřuje na problematiku bezpečnosti cloud computingu ve vztahu k bezpečnosti a auditu.

ISAE *(International Standard on Assurance Engagements)* definuje Komora auditorů České republiky (2011) jako mezinárodní standardy pro ověření zakázky, které se uplatňují při ověření zakázek, ve kterých jde o jiné záležitosti než o audit či prověrky historických účetních informaci.

ISA *(International Standards for Auditing)* definuje Komora auditorů České republiky (2016) jako mezinárodní auditorské standardy, které se uplatňují při auditu historických účetních informací a vztahují se k auditu účetní závěrky. Z pohledu auditu informačních systémů jsou dle Svaté (2011, s. 74) důležité standardy ISA 401, ISA 315 a ISA 330.

- **ISA 401** (Auditování v prostředí počítačových informačních systémů) se zaměřuje na interní kontroly a zavádí pojem **CAAT** *(Computer Assisted Audit Techniques)*, který definuje obecné nástroje pro počítačovou podporu auditu.
- **ISA 315** (Stanovení a vyhodnocení rizik výskytu významné nesprávnosti prostřednictvím znalosti účetní jednotky a jejího prostředí) definuje kontroly nad podnikovým IS/ICT týkající se provozu datového centra, nákupu a údržby programového vybavení, změny programů a zabezpečení. Dále standard definuje aplikační kontroly. Jedná se o manuální nebo automatizované postupy, které mohou mít preventivní nebo detektivní charakter.
- **ISA 330** (Reakce auditora na vyhodnocení rizika) rozděluje testy na dva základní druhy: testy věcné správnosti (navržené k odhalení materiálních nesprávností) a testy kontrol (navržené k testování provozní účinnosti kontrol).

Na mezinárodní auditorské standardy navazuje organizace **INTOSAI** *(International Organization of Supreme Audit Institutions)*, která vydává doporučení pro audit IS/ICT. Jak uvádí Svatá (2011, s. 75), INTOSAI chápe audit informačního systému jako hodnocení interních kontrol, které se člení na obecné kontroly, aplikační kontroly a vývoj systémů. Hodnocení je realizováno pomocí konceptu 3E *(Economy, Efficiency, Effectiveness)*.

Na efektivní řízení rizik je zaměřen framework **COSO ERM** *(Committee Sponsoring Organizations of the Treadway Commission Enterprise Risk Management)*. Jedná se o obecný standard pro řízení rizik aplikovaný mimo jiné i na IS/ICT, který se zabývá aktivitami na všech úrovních organizace: společnost, divize, oddělení. Cíle jsou stanovovány ve čtyřech kategoriích: strategické, provozní, reporting, compliance.

Metodika zahrnuje popis prostředí, stanovení cílů, identifikace událostí, ohodnocení rizik, odpověď na rizika, kontrolní aktivity, informace a komunikace i monitorování. Studie, které souvisí se zavedením COSO ERM a hodnotí možnosti přijetí, popisuje ve svém článku Tavakoli a kol. (2016), který navrhuje nový koncepční rámec pro monitorování výsledků podniku a s tím spojených rizik.

Autoři Rais a Doskočil (2007, s. 69) uvádí, že v případech, kdy byl vyžadován soulad s normou ISO 13335 a ISO 17799, bylo výhodné při analýze rizik využít metodiku **CRAMM** *(CCTA Risk Analysis and Management Methodology)*. Tato metodika byla později dle Risk Analysis Consultants (2017) později nahrazena metodikou **RAMSES** *(Risk Analysis and Management System for Enhanced Security)*, který plně respektuje postupy doporučené řadou norem ISO 27000 a zcela nahrazuje všechny funkcionality metodiky CRAMM. Analýza v rámci těchto nástrojů řeší ohodnocení systémových aktiv, seskupení aktiv do logických skupin, stanovení hrozeb, prozkoumání zranitelnosti a na jejich základě jsou stanovena bezpečnostní opatření.

Stejně jako předchozí dvě metodiky se **OCTAVE** *(Operationally Critical Threat, Asset and Vulnerability Evaluation)* zabývá řízením bezpečnosti a analýzou rizik. Jedná se o soubor metod sloužící pro strategické ohodnocení a plánování informační bezpečnosti na bázi analýzy rizik, které vyvíjí organizace CERT *(Computer Emergency Response Team)*. Dle Koudely (2011) existují tři varianty této metodiky (OCTAVE Method, OCTAVE – S, OCTAVE Allegro), které umožňují zvolit požadovanou verzi v závislosti na konkrétních požadavcích a velikosti organizace.

Další metodika, kterou lze použít pro řízení rizik dle ISACA (2009), se nazývá **Risk IT**. Jedná se o komplexní rámec pro řízení rizik, který integruje různé úrovně rizik a současně je aplikovatelný na rozdíl od výše zmíněných přímo pro oblast IS/ICT. Rámec rozděluje procesy do tří následujících domén: RG *(Risk Governance)*: správa a řízení rizika, RE *(Risk Evaluation)*: hodnocení rizika a RR *(Risk Response)*: reakce na riziko.

Balanced Scorecard představuje systém měření a řízení výkonnosti organizace. Jak dodává Wagner (2009, s. 230–235), zaměřuje se nejen na problematiku měření výkonnosti, ale i na její zasazení do celého systému řízení výkonnosti podniku. Jedná se o obecnou manažerskou metodu používanou často i pro řízení IS/ICT, která převádí cíle

do specifických úkolů, měřítek a ukazatelů. Kaplan a Norton (2010, s. 84–99) zdůrazňují důležitost vyváženého podchycení všech nejdůležitějších skutečností, které určují hodnotu firmy, a znázornění výsledného skóre společnosti, jež se týká hodnocení její výkonnosti. BSC zachovává tradiční finanční měřítka, která vypovídají o minulých finančních transakcích. Tato finanční měřítka jsou ale nevhodná pro stanovení strategie, které si organizace musejí zvolit, aby vytvořily hodnotu. BSC je proto doplňuje o nová měřítka hybných sil budoucí výkonnosti. Cíle a měřítka BSC vycházejí z vize a strategie společnosti a sledují její výkonnost ze čtyř perspektiv: perspektivy finanční, perspektivy zákaznické, perspektivy interních procesů a perspektivy učení se a růstu.

Přístup **Six Sigma** je dle Töpfera (2008, s. 41–49) manažerský koncept založený na pevných datech, který směřuje k odstraňování vad, ztrát nebo problémů v kvalitě produkce. Využívá systematické metody projektového managementu, data a statistické analýzy a snaží se o soustavné měření výkonu podniku a jeho zlepšování za účelem neustálého snižování počtu vad v celém procesu. Veber a kol. (2010, s. 235–236) dále dodává, že koncept Six Sigma je komplexní a flexibilní systém, který napomáhá organizacím k dosažení, udržení a zvyšování jejich výkonnosti a nabízí způsob, jak dosáhnout menšího počtu chyb ve všech jejich činnostech. Cílem této metodiky je produkce výrobků nebo služeb s nižšími náklady, zvýšení spokojenosti zákazníků a zlepšení výsledků organizace. Autorky Pavelková a Knápková (2012, s. 205) také uvádějí, že koncepce Six Sigma svou orientací na neustálé zlepšování výrobků a procesů přispívá k budování excelence a má tedy pozitivní účinky na kvalitu, čas a náklady.

CMMI *(Capability Maturity Model Integration)* představuje procesně orientovaných framework zaměřený na zlepšování procesu vývoje nového produktu. Dle CMMI Institute (2017) je tento framework založen na principu, že kvalita systému a produktu je dána kvalitou firemních procesů. CMMI je definována jako sada „Best practices“, které organizace využívají pro vyhodnocení a zlepšení jejich procesů. Stupňovitý model CMMI definuje 5 úrovní zralosti: Počáteční *(Initial)*, Řízená *(Managed)*, Definovaná *(Defined)*, Kvantitativně řízená *(Quantitatively managed)* a Optimalizující *(Optimizing)*. Celý framework se rozpadá do několika zájmových oblastí, které se specializují určitým směrem: CMMI-DEV *(Product and service development)* se zaměřuje na vývoj služeb a produktů, CMMI-SVC *(Service establishment, management)* na zavádění služeb a jejich

řízení a CMMI-ACQ *(CMMI for Acquisition)* řeší „Best practices“ nákupu produktů a služeb. Na model CMMI je navázáno mnoho akademických studií. Článek autora Crisóstomo a kol. (2016) se zaměřuje na porovnání domény CMMI-DEV and ISO 12207, které spolu úzce souvisí. Další článek autorů Hayata a Qureshe (2016) navazuje na CMMI model a popisuje možnosti zapojení agilních metodik.

Z historických důvodů týkajících se pádu Enronu byl v souvislosti s Corporate Governance vytvořen zákon Sarbanes-Oxley Act neboli **SOX**, který se zabývá průhledností a odpovědností za účetní informace organizací a formuluje nové požadavky na to, jakým způsobem mají společnosti zaznamenávat, sledovat a zveřejňovat svoje finanční informace (The Sarbanes–Oxley Act, 2002). Výchozím počinem zákona, jak uvádí Kovanicová (2007), bylo ustavení **PCAOB** *(Public Company Accounting Oversight Board)* rady pověřené celostátním dohledem nad auditorskou profesí a jejím řízení. SOX zavádí povinnost manažerů a auditorů vyjádřit se k interním kontrolním systémům. Protože rizika v IS/ICT můžou mít velký dopad na finanční výsledky společnosti, finanční auditoři posuzují i informační systémy společnosti.

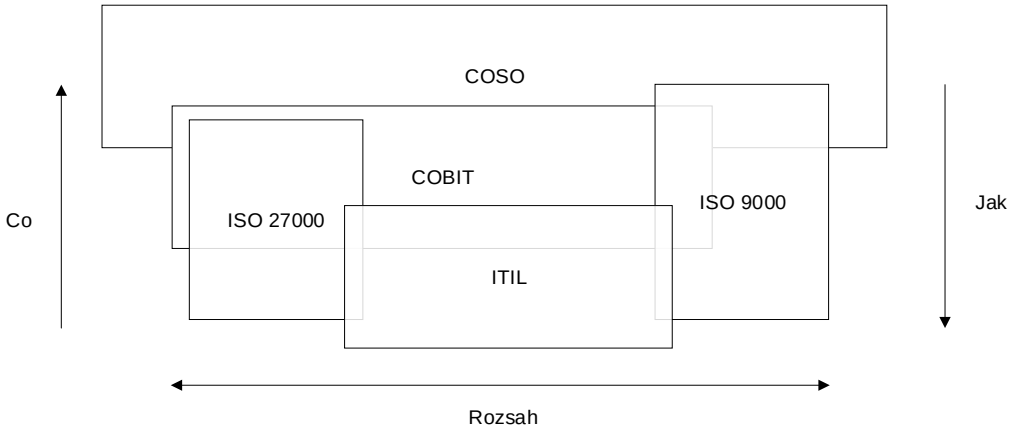
Mezi další dokument, který navazuje na principy Corporate Governance ovlivňuje audit informačních systémů, patří **Basel II**. Tato dohoda, jejíž hlavním cílem je vytváření podmínek pro stabilní bankovní sektor, se dle Jecha (2010) týká především bank a finančních institucí Zabývá se mimo jiné i provozními riziky, která představují selhání interních procesů, lidí a systémů.

Jistý přesah do oblasti hodnocení informačních systémů mají i metodiky PMBOK nebo PRINCE2, které se zabývají projektovým managementem. **PRINCE2** *(Projects in Controlled Environment)* stojí na sedmi principech, tvoří ji sedm procesů a popisuje sedm témat. Doležal a kol. (2012, s. 25) uvádí, že se jedná o procesně orientovaný a strukturovaný standard pro projektový management. Nevěnuje se jen řízení, controllingu, supervizi, designu a organizaci projektu, ale také popisuje, jak v projektu koordinovat účastníky a aktivity. Doležal a kol. (2012, s. 24) dále prezentuje metodiku **PMBOK** *(Project Management Body of Knowledge)* jako procesně orientovaný standard, který popisuje procesy v pěti skupinách: inicializace, plánování, exekuce, kontrola a monitorování a hodnocení projektu. Zabývá se mimo jiné integrací projektu a definuje rozsah, time management, náklady, kvalitu, lidské zdroje, komunikaci, rizika nebo řízení dodávek.

3.2.2 Zhodnocení současného stavu standardů v oblasti řízení IS/ICT

Popsané standardy se liší zejména ve svém rozsahu, který je dán mírou detailu, a primárním zaměření. V přehledu standardů uvedených v předcházející kapitole bylo možné nalézt jak obecné standardy, tak i ty, které se věnují detailům řízení nebo hodnocení jednotlivých procesů. Dále se standardy liší v tom, jestli jsou primárně navrženy pro IS/ICT nebo se do oblasti informačních a komunikačních technologií pouze promítají v rámci řízení jiných procesů. Celkové srovnání všech popsaných standardů je z výše uvedených důvodů problematické. Zhodnocení, které je obsahem této kapitoly, se spíše zaměřuje na porovnání několika přímých konkurentů či nalezení pojítek v metodikách či přístupech, které jsou si na první pohled vzdálené.

Standardy, normy a přístupy COBIT, ISO a ITIL jsou dnes už globální ve smyslu, že je používají firmy na celém světě. Na základě analýzy autorů Sánchez Peña a kol. (2013), Sahibudin a kol. (2008) nebo Gehrmann (2012) a srovnání provedené na COBIT Introductory Workshop (2009) lze zmíněné metodiky graficky znázornit tak, jak je prezentuje obrázek č. 15. Osa x prezentuje rozsah působnosti dané metodiky (ITIL má částečný přesah s rámcem COBIT i s normami ISO 27000 a ISO 9000) a osa y míru detailu (COSO je ve srovnání s metodikou ITIL spíše obecné a ITIL více konkrétní).



Obrázek 15: Grafické porovnání metodik a přístupů COSO, COBIT, ITIL, ISO 9000 a ISO 27 000 (COBIT Introductory Workshop, 2009)

Podobné srovnání lze vyjádřit i pomocí jiných kritérií, která prezentuje ve svých článcích například autor Haufe a kol. (2016) a objevuje se také na COBIT Introductory Workshop (2009). Srovnávané jsou standardy COBIT. ITIL a ISO 27000 na základě pěti kritérií:

funkce, oblasti, vydavatel, certifikace a zaměření. Kritérium funkce popisuje hlavní orientaci dané metodiky, oblasti pak definují, na jaké části je metodika členěná. Dále jsou v tabulce uvedené informace o zaměření každé metodiky a příslušný vydavatel.

Tabulka 3: Srovnání standardu COBIT, doporučených přístupů ITIL a normy ISO 27000 (COBIT Introductory Workshop, 2009; Haufe a kol., 2016)

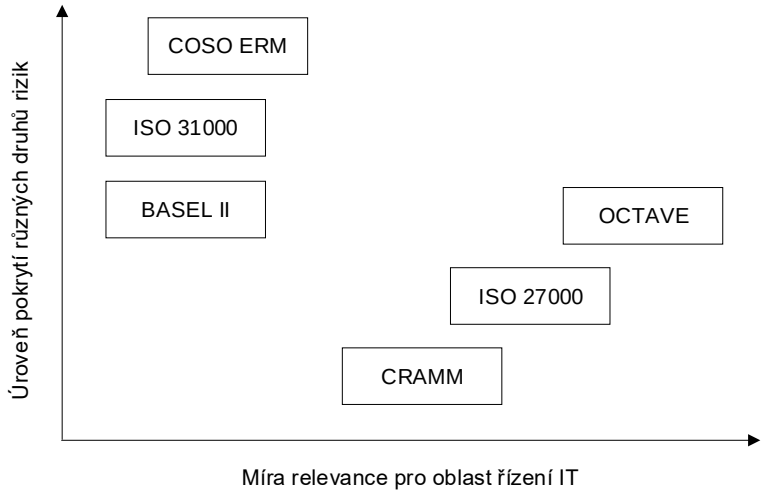
Standard	Funkce	Oblasti	Vydavatel	Certifikace	Zaměření
COBIT	Mapování IT procesů.	4 procesy 34 domén	ISACA	Bez certifikace.	IT Governance nebo audit informačního systému.
ITIL	Mapování služeb informačních technologií.	9 procesů	OGC	Certifikace zaměstnanců.	Řízení služeb v IS/ICT.
ISO 27000	Řízení rizik v oblasti informační bezpečnosti.	10 domén	ISO	Certifikace organizace.	Shoda s normou.

K dalším standardům, které byly popsány v předchozí kapitole, patří rámce pro řízení procesů CMMI či standardy ISO pro řízení programového vybavení. Standard ISO 15504 je známý referenční model softwarového procesu ISO 12207, který se od normy oddělil při její revizi v roce 2004. ISO 15504 se po oddělení ISO 12207 zaměřuje na posouzení kvality procesu a je tak základem pro práci auditorů, nikoli pomůckou pro softwarové týmy. Principy prezentované v CMMI jsou velmi blízké těm, které jsou známé v jiných metodologiích od ITIL po ISO. Model CMMI se u ISO 15504 a ISO 12207 inspiruje, takže jsou oba modely velmi podobné a vzájemně kompatibilní. V literatuře lze nalézt odkazy na slovníky a pomocné postupy pro zachování vzájemné kompatibility, které zavádí a prezentuje ve svých publikacích např. autor Crisóstomo a kol. (2016).

Z pohledu auditu informačních systémů se jeví jako výhodné použít IT Assurance Guide a v případě auditu velké společnosti je to jistě správná volba. Z důvodu komplexnosti celého dokumentu je ale problematické tuto metodiku použít na menší audit. Dle Svaté (2011, s. 100) vyžaduje aplikace IT Assurance Guide od auditorů velkou schopnost vymezit a ohraničit předmět projektu ujištění a následně vybrat doporučené kroky jednotlivých kontrol, které budou přínosem v kontextu podnikových procesů.

K dalším standardům věnujícím se konkrétním oblastem patří Val IT, který poskytuje odpověď na to, zda investice do IT projektů jsou správné a jestli přináší požadovaný výnos. Risk IT společně s Val IT a COBIT představuje velmi provázený model kontrol, investic a rizika pro oblast řízení a poskytování služeb v IS/ICT.

Pro oblast řízení rizik v rámci IT Governance existuje také mnoho standardů a metodik. Po hlubší analýze lze identifikovat, že některé z nich se zabývají především podnikatelskými riziky (COSO, ISO 31000 nebo BASEL II) nebo především bezpečností IS/ICT (OCTAVE, ISO 27000, CRAMM/RAMSES). Nástroje se také velmi liší náklady na pořízení a provoz, náročností implementace či podpůrným programovým vybavením. Porovnání rámců dle míry relevance pro IS/ICT a úrovni pokrytí rizik ilustruje obrázek č. 16.



Obrázek 16: Porovnání rámců pro řízení rizik (Information Security Forum, 2010)

Do řízení a hodnocení informačních systémů a s nimi spojených procesů se promítají i některé standardy, které nejsou přímo určeny pro IS/ICT. Například zmíněné COBIT, ISO 27000 nebo Val IT jsou standardy vysloveně určené pro řízení informatiky ve firmě a lze tedy podle nich IS/ICT řídit samostatně. Naproti tomu Balanced Scorecard nebo Six Sigma jsou rámce, které bývají obvykle přijaty na obecné podnikové úrovni s tím, že je pak snaha jim v určitých oblastech podřídit i IS/ICT. Možným propojením přístupů Six Sigma a Balanced Scorecard se věnují autorky Pavelková a Knápková (2012, s. 205). Zkombinováním strategického pohledu Balanced Scorecard a operativního přístupu Six Sigma může být využito přínosů obou těchto modelů. Využitím přístupu Balanced Scorecard pro hodnocení informačního systému se zabývá Kim a kol. (2012).

3.3 Současný stav poznání v oblasti hodnocení informačních systémů

Cílem kapitoly je vytvořit souhrnný popis vývoje i současného stavu v oblasti hodnocení informačních systémů.

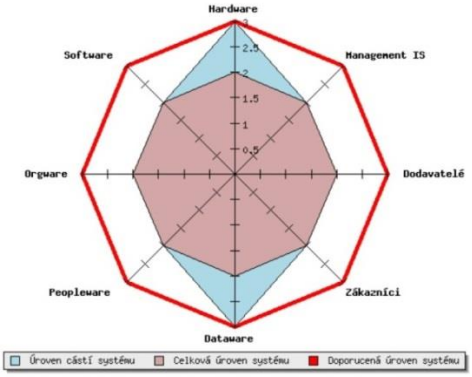
Pro posouzení stavu informačních systémů lze přímo či nepřímo použít mnoho analýz. Některé z nich jsou cíleny přímo na několik dílčích charakteristik podniku, jiné jsou šity na míru pro potřeby posouzení informačních systémů. Na základě získaných výsledků je možné si rozšířit obzory a nalézt do budoucna nové oblasti zkoumání. Tyto analýzy mohou být užitečné například pro tvorbu informační strategie, která zahrnuje návrhy pro systematické plánování informačních systémů a technologií.

Metodiky a rámce, které jsou popsány v této kapitole, pracují na podobných základech, mnohdy i s obdobnými kritérii, přesto ne všechny si konkurují. Obvykle jsou totiž cíleny na konkrétní část životního cyklu informačního systému nebo na dodávku specifického řešení. Proto je možné metodiky použít zároveň v případě různých řešení konkrétního modelu (jeden zkoumá finanční kritéria a druhý názory uživatelů) nebo za sebou v případě hodnocení různých životních fází informačního systému.

3.3.1 Přehled publikací zaměřených na hodnocení informačních systémů

Pomocí metodiky **HOS8**, která byla vytvořena na Fakultě podnikatelské VUT v Brně, lze posoudit informační systém firmy podle osmi klíčových oblastí a lze tak zjistit, zda jsou tyto oblasti na podobné úrovni. HOS8 vznikla na základě metodiky **HOS** z roku 1998 v duchu následující myšlenky: pokud je jedna ze zkoumaných částí nevyvážená, vede to k neefektivitě celku. Úroveň systému je dána právě nejslabším článkem. Na rozdíl od metodiky **ZEFIS**, kterou se zabývám v jednom z následujících odstavců, je prováděno posouzení informačního systému na základě jednoho dotazníku vypracovaného manažerem firmy. Pro hodnocení se používá číselná stupnice 1 až 4, kde vyšší číslo představuje lepší stav zkoumané oblasti. Za vyvážený systém je pak považovaný takový informační systém, kde všechny osy mají stejné hodnocení, nebo nejvýše tři z nich se odlišují od ostatních nejvýše o hodnotu. Celková úroveň systému je v grafu zakreslena světle červenou barvou. Doporučený stav je dán přikládanou důležitostí firmy na systém, který je ohraničen tmavě červeně. Na základě získaných výsledků je možné zvolit několik protiopatření. Na této metodě postupně pracovali Kříž (2001), Dovrtěl (2004), Koch (2005) a Neuwirth (2009).

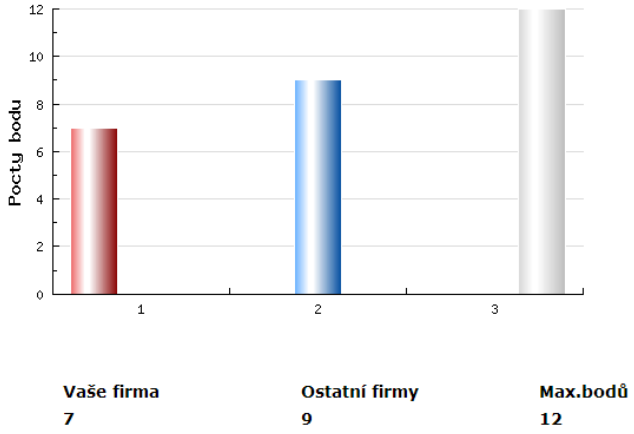
K oblastem zkoumání metodiky **HOS** patří dle Kříže (2001) a Dovrtěla (2004) hardware, software, orgware, peopleware, dataware, zákazníci, dodavatelé a management. Zkoumá se tedy postupně technické a programové vybavení, pracovní postupy a pravidla, postupy zaměstnanců, správa dat a aspekty informační strategie. Za zákazníka informačního systému může být kromě externího zákazníka považován i interní pracovník, který systém potřebuje ke své práci. Jako dodavatel je označen ten, kdo se stará o provoz, tedy interní nebo externí pracovník. Poslední aktualizací této metodiky podle Neuwirtha (2009) je **HOS2009**, která se snaží o odstranění slabých míst metodiky **HOS8**, které byly odhaleny jejím praktickým využíváním. Současné oblasti zkoumání byly doplněny o bezpečnost a management informačního systému.



Obrázek 17: Posouzení vyváženosti informačního systému firmy (Koch a kol., 2010)

Metodika **ZEFIS** slouží pro online posuzování informačních systémů. Stěžejní část tvoří možnost srovnání zadaných dat především s českými a slovenskými společnostmi. Systém, jejímž autor je Koch (2014), byl postaven zejména pro menší firmy, které potřebují vědět, zda jsou jejich informační systémy dostatečně efektivní a chtějí mít možnost porovnat úroveň svých systémů a jejich řízení s ostatními firmami. Průzkum probíhá pomocí vytvořených dotazníků a výsledky z nich plynoucí jsou dostupné ihned po zadání a zdarma. Systém dokáže srovnat data z dotazníků se zmíněnou databází firem a na základě výstupů je možné posoudit, zda vybrané oblasti podnikového systému jsou lepší či horší než u ostatních firem a na základě toho vyvodit příslušná opatření. Odpovědět na otázky v dotaznících lze výběrem jedné z nabízených možností a v několika případech je povoleno zvolit více odpovědí. Ve fázi vyhodnocení průzkumu je možné zvolit, s jakými firmami budou porovnávány výsledky dle velikosti firmy a oblasti podnikání. Jako další kritérium je definována pracovní pozice zaměstnance, podle

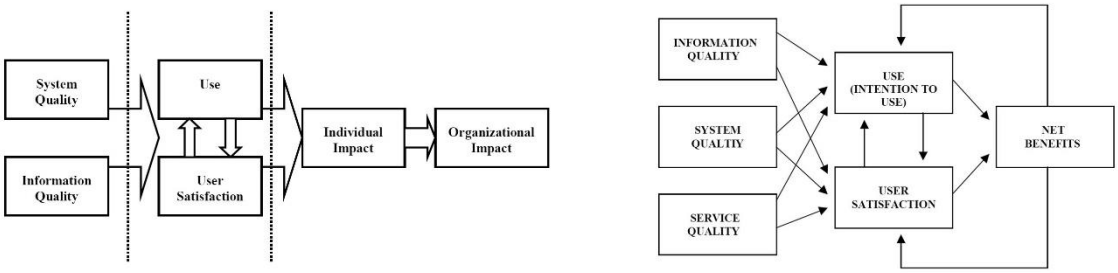
níž lze dotazníky také třídit. Autor dále dodává, že samotné vyhodnocení je rozděleno do osmi základních kapitol, kdy každá kapitola popisuje jednu z následujících dimenzí: např. informační systém, pracovníci, úroveň podpory, efektivnost atd. V každé kapitole jsou uvedeny klíčové oblasti, které byly zkoumány, a nejčastější odpovědi respondentů srovnané s pracovníky ostatních firem. V závěru každé strany jsou uvedena shrnutí a doporučení. Dále je možné procházet a analyzovat jednotlivé odpovědi ve všech shromážděných dotaznících. Lze také porovnat vložené odpovědi respondentů a odpovědi pracovníků ostatních vybraných firem.



Obrázek 18: Srovnání firem dle výsledků v metodě ZEFIS (Koch, 2014)

Již v roce 1992 byl představen **The DeLone and McLean Model of Information Systems Success Model**, který poskytuje prostředek pro komplexní hodnocení informačních systémů. Autoři DeLone a McLean (1992) identifikovali čtyři kategorie, podle kterých jsou systémy hodnoceny: kvalita systému, kvalita informací, užití informací a spokojenost uživatelů. Jedenáct let po uvedení první verze autoři DeLone a McLean (2003) model aktualizovali a vylepšili s ohledem na nové podmínky na trhu. Jedná se například o měření efektivity e-commerce systémů. Práce obsahuje také řadu doporučení týkajících se použité metodiky měření. V konceptuálním modelu efektivnosti informačních systémů je měření postaveno na faktu, že efektivnost je založena na spokojenosti uživatelů. Tato premisa je dále rozvinuta v prostředí e-commerce a obohacena o nový typ uživatelů, tzv. e-zákazníků. Z tohoto pohledu lze pak nalézt přímou souvislost mezi hodnocením spokojenosti e-zákazníka a hodnocením kvality služeb. V souvislosti s výše zmíněným pak podle této studie není vhodné využít již zavedené nástroje, které měří spokojenost uživatelů informačních systémů. Proto se autoři rozhodli,

v návaznosti na komplexní studia literatury, odvodit vhodný model pro zkoumání a měření spokojenosti e-zákazníků. Na základě tohoto modelu postupovali např. Pather a kol. (2003) nebo Hosnavi a Ramezan (2010), kteří prezentovali svou studii v příspěvku s názvem **Measuring the effectiveness of a human resource information system in National Iranian Oil Company**. Výsledkem práce bylo vytvoření metodiky pro hodnocení pomocí dotazníkového šetření s 28 otázkami zaměřenými na uživatele informačního systému.



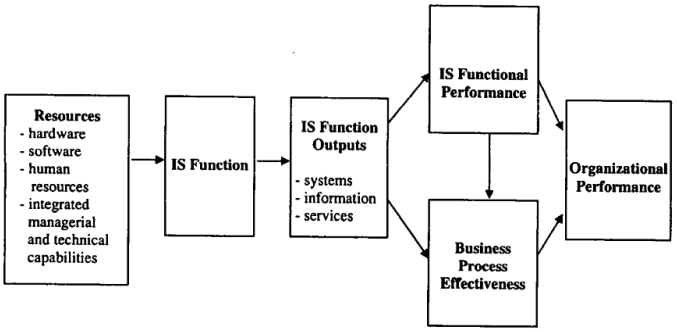
Obrázek 19: Model z roku 1992 a jeho aktualizace z roku 2003 (DeLone & McLean, 2003)

Bohuslav a Basl (2003) ukazují ve své práci **Inovace podnikových informačních systémů** aplikaci inovačních řádů na informační systémy. Hned od počátku autoři rozdělili pohled na inovace informačního systému na dvě části: pohled podniku (zákazníka) a pohled dodavatele. V článku je navržena metodika pro hodnocení podniku v jednotlivých oblastech řízení informatiky. Těmito oblastmi jsou funkcionalita informačního systému, řízení IT, procesy v IT, lidé, informační a komunikační technologie, data a SW podpora rozhodování. Autoři také vyzdvihují, že pokud se inovace dotkne pouze jediné oblasti, tak dojde ke zlepšení celého informačního systému.

Sodomka (2002) ve své práci **Hodnocení efektivnosti ERP systémů** popisuje rozpor mezi pohledem uživatelů a dodavatelů informačních systémů na jejich efektivnost. Definuje kritické faktory efektivnosti a klíčové oblasti, mezi které řadí strategii a řízení firmy, zaměstnance, připravenost organizace a proces implementace ERP. Výsledky šetření pak je možné získat pomocí řízeného interview dvojice dodavatel-odběratel.

Autoři Cha-Jan Chang a King (2005) se ve své studii **Measuring the Performance of Information Systems: A Functional Scorecard** zabývají vývojem nástroje, který může být použitý k posuzování informačních systémů na základě ohodnocení pomocí skórkarty. Je založen na teoretickém modelu funkčních rolí informačního systému, jehož

cílem je podporovat firemní procesy a výkonnost organizace. Metodika se skládá ze tří výstupních dimenzí: výkon systému, informační efektivnost a úroveň podpory. Pro vývoj a testování schématu byly využity data od 346 uživatelů ze 149 firem. Tento proces vyústil v nástroj, který měří 18 faktorů v rámci již zmíněných dimenzí. Následně byla metodika testována pomocí dotazníkového šetření mezi 120 uživateli a výsledky ukázaly, že použitá metodika opravdu poskytuje prostředky pro zlepšení efektivnosti obchodních procesů. Navržený nástroj se tak může využít nejen k ohodnocení informačních systémů, ale také lze na jeho základě rozhodnout o budoucích finančních investicích do IS/ICT.

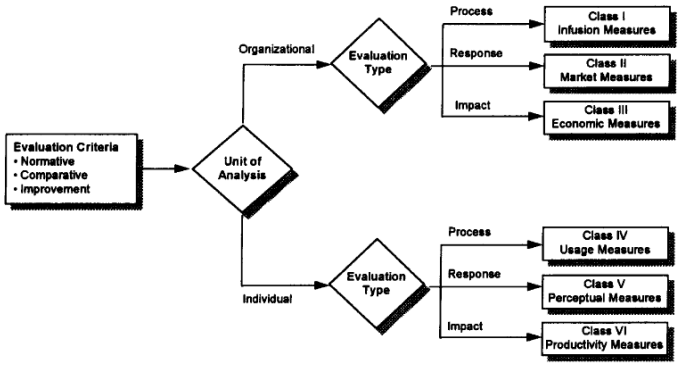


Obrázek 20: Model výkonnosti informačních systémů (Cha-Jan Chang & King, 2005)

K **Měření ekonomické efektivnosti informačního systému** lze podle Maryšky (2007) využít systémy pro hodnocení nebo i jednoduché a složené ukazatele např. ROI, dobu návratnosti, BSC a CPM. Při této metodě posuzování je kladen důraz zejména na stanovení požadavků na měření a popsání všech ukazatelů pro budoucí potřebu. Všechny skupiny ukazatelů mají své kladné a záporné stránky. Hodnotitel si musí na základě svých požadavků určit, které z ukazatelů budou splňovat jeho požadavky nejlépe. Není možné obecně říci, který z přístupů (natož pak ukazatelů) použít.

Podkladem práce **Information systems effectiveness: The construct space and patterns of application**, kterou publikoval Grover a kol. (1996), jsou již vyvinuté a empiricky testované metodiky. Autoři pak na jejich základě definovali kritéria pro hodnocení informačních systémů, které od počátku sledovali z makro (organizace) a mikro (uživatel) pohledu. Studie zapadá do kontextu ostatních prací na podobné téma s tím rozdílem, že zde jsou definovány domény efektivnosti a třídy výkonnostních kritérií. V práci jsou navrhnuty tři typy ohodnocení: proces (za předpokladu, že při omezených zdrojích pracují zaměstnanci tak, aby je efektivně využili – hodnotí se na

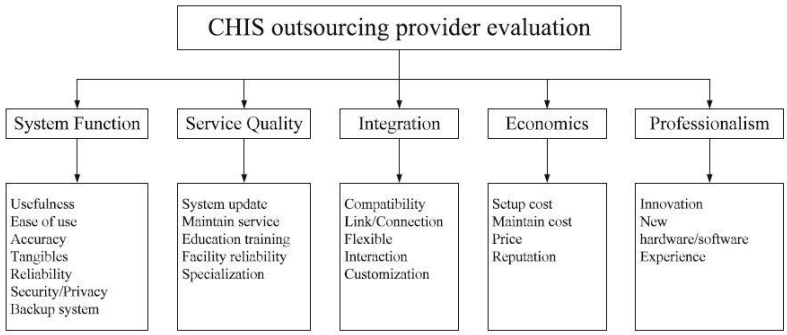
základě uživatelské závislosti na informační systém), odezva (měření pozitivních a negativních hodnocení uživatelů) a dopad (dopad zásahu na zaměstnance nebo celou organizaci). Dále je popsáno šest tříd měření, která jsou následně promítnuta v různých kontextech hodnocení. Nástroje a příklady užití vyvinuté v rámci této studie poskytují nový způsob konceptualizace a rozšiřují použití mnoha hodnotících kritérií, která jsou spojena s informačními systémy.



Obrázek 21: Metodika pro posouzení informačních systémů (Grover a kol., 1996)

Autoři Low a Chen (2012) se ve své studii **Criteria for the Evaluation of a Cloud-Based Hospital Information System Outsourcing Provider** zabývají výběrem kritérií pro posouzení dodavatele nemocničního informačního systému, který je založen na Cloud computingu. Poukazují, že integrací činností, které jsou spojeny s péčí o pacienty, administrativním řízením a systémem zdravotní péče se může zvýšit výsledná efektivnost nemocničního informačního systému. Právě tuto integraci nabízejí cloudové informační systémy, ve kterých je pro lékaře snazší přistupovat k záznamům pacienta z několika nemocnic. Výběr poskytovatele outsourcingu představuje vícekriteriální rozhodovací proces, který pracuje s rozdílnými cíli, jako jsou náklady, kvalita nebo rychlost. Autoři v této práci navrhli hodnotící model založený na metodách FDM *(Fuzzy Delphi Method)* a FAHP *(Fuzzy Analytic Hierarchy Process)*, které lze využít pro multikriteriální rozhodovací úlohy. Hodnocení systému probíhá ve třech krocích. V první fázi autoři definovali na základě předchozích výzkumů 28 dimenzí, které roztřídili do 5 kategorií: funkce systému, kvalita systému, integrace, ekonomika a profesionalita. Pro ověření autoři rozeslali 300 dotazníků s cílem potvrdit si od zaměstnanců pracujících v nemocnicích na manažerských a IT pozicích, která kritéria jsou při výběru informačního systému pro nemocniční personál důležitá. Ve druhé fázi požádali autoři 42

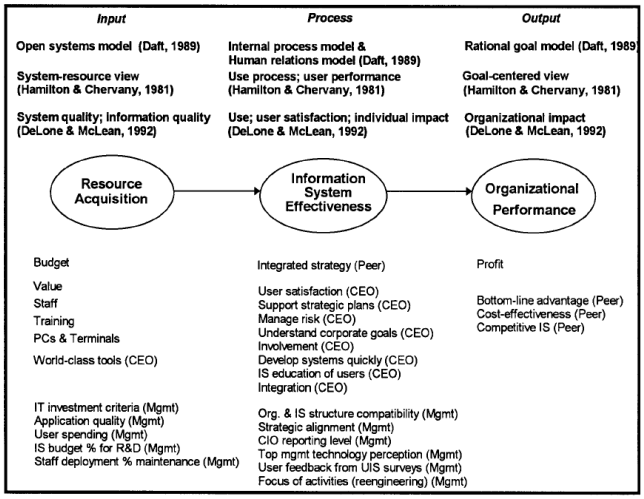
expertů z oblasti IT, aby ohodnotili důležitost (váhu) jednotlivých dimenzí. Ve třetí fázi byly dimenze seřazeny podle důležitosti. Výsledkem práce je třístupňový model. První stupeň představuje celkové hodnocení dodavatele *(CHIS outsourcing provider evaluation)*. Ve druhé úrovni je pět dimenzí, které zastřešují dohromady 24 kritérií ve třetím stupni.



Obrázek 22: Třístupňový model ohodnocení dodavatele cloudového IS (Low & Chen, 2012)

Autor Botchkarev a kol. (2011) ve svém článku **A Return on Investment as a Metric for Evaluating Information Systems: Taxonomy and Application** nabízí různé pohledy na využití ukazatele rentability vloženého kapitálu ROI společně s příklady z oblasti posuzování informačních systémů. Autor v článku předkládá různé varianty použití ukazatele: tradiční ROI *(Traditional ROI)*, rozšířené ROI *(ROI Extensions)* a virtualizace ROI *(ROI Virtualizations)*. Pro hodnocení konkrétní investice je možné zvážit použití jedné z těchto tří zmíněných možností. Tradiční ROI *(Traditional ROI)* se počítá ve skutečných peněžních jednotkách a retrospektivně. Účetní záznamy jsou používány jako zdroj dat pro výpočet – kvalita výpočtu závisí na kvalitě zdrojových dat. Výdaje zahrnují vše, co souvisí s investicí. Zisk z investice může být složen např. z úspory nákladů na pracovníky (uspořené peníze může společnost fyzicky využít k jinému účelu) nebo zvýšení tržeb. Rozšířené ROI *(ROI Extensions)* se počítá na rozdíl od tradičního ROI pro ohodnocení budoucích projektů a je zde již zahrnuta časová hodnota peněz a dopady rizik. Pro výpočet se používají stejné druhy nákladů i výnosů a je zachován i stejný vzorec. Z účetních výkazů ale nelze získat náklady a přínosy pro budoucí projekty. Výhodou metody Virtualizace ROI *(ROI Virtualizations)* je zahrnutí nehmotných výnosů či přínosů, které jsou ale obtížně měřitelné a není vždy jednoduché jim přiřadit peněžní hodnotu. Může k nim patřit např. lepší informace, efektivně zvládnuté procesy, produktivita, vzdělání zaměstnanců nebo spokojenost zákazníka.

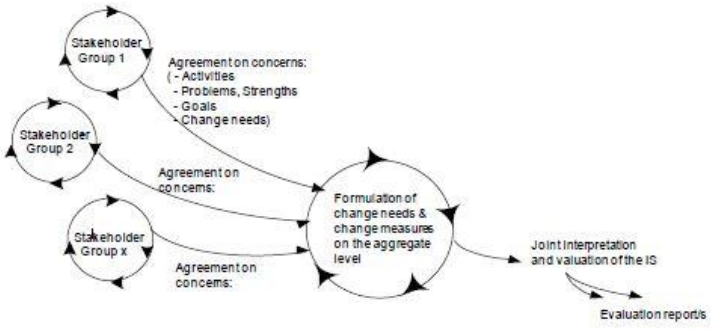
Práce s názvem **The Measurement of Information Systems Effectiveness: Evaluating a Measuring Instrument**, (Scott, 1995), se zabývá problematikou měření specifických částí informačního systému a dopadem na jeho efektivnost. Snahou autora je potvrdit ohodnocení, které proběhlo v rámci žebříčku Computerworld Premier 100. K měření efektivnosti informačních systémů autor využil matematické rovnice, v práci jsou však také uvedeny návrhy na alternativní měřící nástroje. Na základě získaných výsledků vyvstaly pochybnosti se spolehlivostí a platností tohoto měření. Je totiž problematické kombinovat do jedné rovnice více proměnných heterogenního charakteru. Východiskem z tohoto problému byla změna pohledu na efektivnost informačních systémů jako na multidimenzionální prostor, jehož implementace je součástí tohoto modelu. Měření probíhá v této metodě v následujících skupinách: rozpočet, kvalita informací, zaměstnanci, trénink, PC a terminály, zisk, sdílení informací. Na základě předchozích výzkumů v této oblasti jsou také v práci nabízeny návrhy na zlepšení měření.



Obrázek 23: Framework pro posuzování efektivnosti informačních systémů (Scott, 1995)

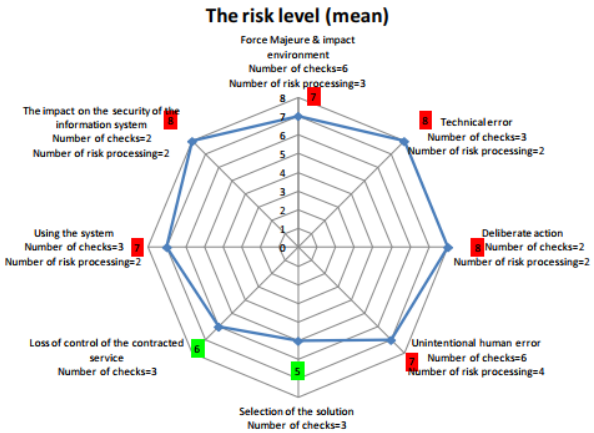
Hlavním cílem autorky článku **Evaluating Information Systems according to Stakeholders: A Pragmatic Perspective and Method**, který publikovala Lagsten (2011), bylo vypracovat metodu sloužící k hodnocení informačních systémů zainteresovanými stranami (stakeholders) zaměřenou na změnu a zlepšení současného stavu. Výsledkem studie byla metodika VISU, která je určena pro praktické použití ve firemním prostředí. Metodika byla vytvořena a testována v šesti po sobě jdoucích cyklech: hodnotící model, vytvoření hodnotících procesů, teoretická východiska hypotézy modelu, popis metodiky, hodnotící proces pomocí stakeholders a výsledky použití metodiky.

V každém cyklu byly definovány výzkumné otázky a bylo představeno jejich řešení. Autor dále definuje, že mezi teoretické opory metodiky VISU patří především tříúrovňový model, který dává do souvislosti hodnoty, cíle, akce a dopady těchto akcí. Hlavní cíl metodiky VISU je shrnout zájmy všech uživatelů informačního systému pomocí systematických dialogů. Proces hodnocení se provádí ve třech fázích: organizovat a zařídit *(Arrange)*, posoudit a hodnotit *(Evaluate)* a rozvíjet *(Develop)*. VISU umožňuje hodnotitelům převzít zodpovědnost za celý proces hodnocení. To je důležité, protože první fáze *(Arrange)* má do značné míry vliv na to, jak později budou výsledky hodnocení použity ve třetí fázi *(Develop)*.



Obrázek 24: Hodnotící proces dle metodiky VISU (Lagsten, 2011)

Autor Solic a kol. (2015) ve své práci **The information systems' security level assessment model based on an ontology and evidential reasoning approach** navazuje na předchozí výzkum v této oblasti a navrhuje model, který může být základem nového řešení pro vyhodnocování bezpečnosti informačních systémů. Toto řešení je schopno pokrýt širokou škálu všech možných otázek zabezpečení informací. Model je založen na znalostní bázi a k vyhodnocení používá matematický algoritmus.



Obrázek 25: Výsledek hodnocení metodiky (Solic a kol., 2015)

3.3.2 Zhodnocení současného stavu vědeckého poznání

Autoři metod obvykle zakládají své představy o hodnocení informačních systémů na podobných základech. Obecně se všechny zabývají podnikem a jeho okolím. Pozorovaným subjektem je obvykle uživatel informačního systému a efektivnost je hodnocena pomocí dotazníku např. (Dovrtěl, 2004), (Koch, 2005) nebo (Neuwirth, 2009), interview (Lagsten, 2011) a (Hosnavi & Ramezan, 2010) či skórkarty (Cha-Jan Chang & King, 2005). Hodnocení provádí jeden (Koch, 2005) nebo více respondentů (Lagsten, 2011). Autoři se shodují, že pro zkoumání informačních systémů je nutné zahrnout více oblastí zkoumání, např. IT management, kvalita informací nebo spokojenost uživatelů. Kritéria jsou obvykle v souladu s prací autorů Delone a McLean (2003). V počtu či přesné obsahové struktuře se však rozchází. Metodiky jsou si proto navzájem podobné, nikoli však totožné.

Někteří autoři také ve svém výzkumu zahrnují rozpor mezi dodavateli a uživateli informačního systému např. (Sodomka, 2002) a (Bohuslav & Basl, 2003) nebo přímo rozlišují hodnocení zaměřené na uživatele a celou organizaci (Grover a kol., 1996). Dále je u některých metod možné výsledky srovnat s konkurencí nebo automaticky obdržet doporučení pro zlepšení aktuálního stavu (Koch, 2014) nebo (Neuwirth, 2009). Hodnocení je podle některých autorů možné provést výhradně pomocí izolovaných finančních ukazatelů (Maryška, 2007), (Botchkarev a kol., 2011) a (Wachnik, 2012) nebo je možné ukazatele dále zapracovat do komplexní matematické funkce s číselným výstupem (Low & Chen, 2012) a (Scott, 1995).

Autoři Low a Chen (2012) se zabývali počtem a obsahovou náplní kritérií pro hodnocení dodavatele informačního systému. Model je zaměřený pouze na výběr a posouzení systému a dodavatele a pokrývá tedy jen druhou fázi životního cyklu: výběr systému a implementačního partnera dle Sodomky a Klčové (2010, s. 93–97). Práce nepřináší konkrétní zpracování dotazníku pro hodnocení kritérií, jejím cílem bylo zjistit počet kritérií a jejich váhu pomocí dotazníkového šetření mezi experty. V práci není definován postup, jakým způsobem hodnotit zmíněná kritéria. Kritéria jsou zaměřena jen na dodávku pomocí cloud computingu, jiné modely dodávky autoři neuvažovali. Po úpravě některých kritérií by ale bylo možné metodu využít i pro jiný model dodávky.

Autor Botchkarev a kol. (2011), který použil návratnost investic jako metriku pro hodnocení informačních systémů, nabízí ve své práci pouze ekonomický pohled. V případě hodnocení informačního systému pouze pomocí metriky ROI se sleduje jen jedno kritérium, a proto lze tento ukazatel velmi těžko využít při komplexním hodnocení. Naopak ho lze ale uplatnit ve více fázích životního cyklu informačních systémů. Výpočet ROI je individuální a má význam pouze v rámci řešení jednoho problému, který má vždy své specifické náklady a výnosy. Existují různé přístupy k výpočtu ukazatele ROI, výsledky jsou proto často navzájem nekompatibilní a nelze je porovnávat. Každý výsledek výpočtu je třeba podrobit další analýze, protože i projekty s negativním výsledkem ROI mohou být úspěšně realizovány, např. v případě, že investice umožní rozšířit tržní příležitosti firmy.

Hodnocení informačních systémů podle stakeholders (Lagsten, 2011) lze použít, pokud je informační systém již implementovaný. Metodika je zaměřena na ohodnocení současného stavu a implementaci změn. Při aplikaci této metodiky je důležité, aby v roli hodnotitele byl odborník, který disponuje informacemi a znalostmi o používání, vývoji a zatížení systému. Stejné podmínky je možné pozorovat i u (Dovrtěl, 2004). Přenesení výsledků výzkumu do praxe musí být velice citlivé, je nutné analyzovat, zda nedojde změnou k ohrožení práce jiné zainteresované skupiny. Ještě před implementací změn je nutné analyzovat vazby mezi skupinami, protože každá skupina má při práci s informačním systémem jiné problémy a jiné cíle.

Do komparativního porovnání metod, které prezentuje tabulka č. 4, byly vybrány metodiky pro hodnocení informačních systémů splňující následující kritéria: vědecký článek detailně popisuje použití metodiky a zároveň předkládá návod použití nebo případovou studii s výsledy hodnocení. Celkem osm metodik bylo zahrnuto do srovnání, které na posledním řádku tabulky prezentuje také metodiku, jež je předmětem této dizertační práce a byla publikována v článku v roce 2016. Porovnání bylo vytvořeno na základě použité vědecké metody, oblasti (definuje, jak je metodika členěná) a fáze životního cyklu informačního systému. Dále výstupu metodiky a doporučení (definuje jaká je forma výstupu a zda je součástí výstupu také doporučení pro zlepšení), možnosti srovnání mezi podniky (zda lze výsledky porovnávat mezi podniky) a primárního zaměření (velikost společností a obor podnikání).

Tabulka 4:Přehled a popis dimenzí

Název metodiky a autoři	Použité metody	Oblasti	Fáze životního cyklu informačního systému	Výstup metodiky a doporučení	Srovnání mezi podniky	Primární zaměření
Low & Chen (2012)	Dotazníková metoda a Fuzzy Delphi Method	3 fáze / 28 kritérií rozdělených v 5 kategoriích	Výběr informačního systému a dodavatele řešení	Číselná hodnota / Ne	Částečně (lze porovnávat v rámci jednoho projektu)	CHIS (Cloud-based Hospital IS)
Botchkarev a kol. (2011)	Metodika hodnocení investic (ROI)	1 kritérium, 3 možnosti využití	Použitelné pro více fází životního cyklu informačního systému	Číselná hodnota / Ne	Částečně (závislé na podmínkách hodnocení)	Nezávislé na prostředí
VISU Lagsten (2011)	Řízené interview	3 fáze, obsah kritérií je částečně závislý na projektu a zadavateli	Posouzení současného stavu informačního systému a implementace změn	Report / Ne	Částečně (v rámci jednoho projektu, hodnocení jsou velmi subjektivní)	Malé, střední a velké firmy
ZEFIS Koch (2014)	Kombinace dotazníkové metody a interview	6 fází	Posouzení současného stavu informačního systému	Report / Ano (základní)	Ano	Pouze malé firmy
HOS2009 Neuwirth (2009)	Dotazníková metoda	10 dimenzí	Posouzení současného stavu informačního systému	Číselná hodnota a report / Ano (základní)	Ano	Pouze malé firmy
Cha-Jan Chang & King (2005)	Dotazníková metoda	3 dimenze a 120 kritérií	Posouzení současného stavu informačního systému	Report / Ne	Částečně	Malé, střední a velké firmy
Solic a kol. (2015)	Dotazníková metoda, hodnocení pomocí ontologie	3 dimenze	Posouzení současného stavu informačního systému	Číselná hodnota / Ne	Ano	Malé, střední a velké firmy
Novák (2016)	Kombinace dotazníkové metody, studia dokumentů a interview	4 dimenze, 6 fází	Posouzení současného stavu informačního systému	Report / Ano (podrobné, na základě databáze nedostatků)	Ano (částečně ovlivněno kvalitativním charakterem vyhodnocení)	Malé, střední a velké firmy

3.4 Závěry ke stávající praxi hodnocení informačních systémů

Poslední kapitola v oblasti současného stavu vědeckého poznání stručně shrnuje nedostatky současného vývoje používaných metodik a rámců v oblasti hodnocení informačních systémů a na tomto základě vymezuje východiska pro návrh nové metodiky hodnocení informačních systémů, kterému se detailně věnuje kapitola 4.

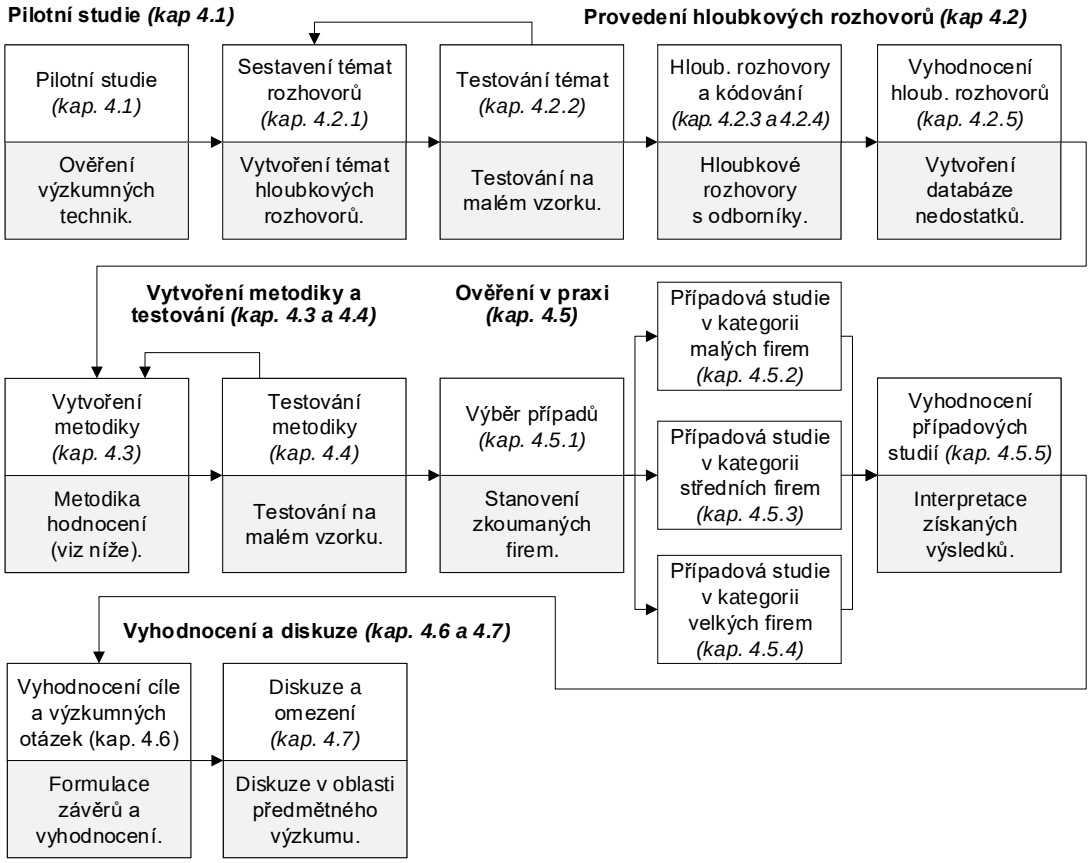
Každý podnik je specifický a zavádění opatření směřující ke zlepšení musí být provedeno s citem k již vytvořeným pravidlům a postupům dané organizace. Z tohoto faktu vyplývá, že pro zavedení jakéhokoli zlepšení neexistuje pouze jeden správný akční plán. Pro účel řízení informačních systémů vznikla řada norem, ve kterých se zavádí pojmy, definice, seznam postupů a návodů a mnoho dalšího pro zvládnutí celé problematiky. Na rozdíl od metodik úzce zaměřených na jeden proces či téma, které se zabývají hodnocením rizik (CRAMM, RAMSES), projektovým managementem (PRINCE2), kvalitou (Six Sigma) nebo hodnotou IS/ICT (Val IT), je východiskem této práce navázat na metodiky zaměřené na komplexní hodnocení. COBIT se ale zdá až příliš obsáhlý a zaměřený především na velké firmy a metodiky HOS či ZEFIS zase přichází spíše s jednoduchým modelem pro malé podniky. Výsledky metodiky VISU jsou kvůli zapojení řízených interview až příliš subjektivní a prověření systémů pomocí IT assurance guide se zdá být příliš robustní a náročné. Některé metodiky navíc definují jen výslednou číselnou hodnotu hodnocení a nepřináší žádné detaily týkající nápravných postupů. Obecně převládají tyto nedostatky: zaměření pouze na určité spektrum firem, procesů či systémů, nejednoznačné výsledky (není možné jednoduše identifikovat nedostatky a získat možná opatření), neaktualizované (zahrnující již nedoporučovaná opatření), nákladné na zavedení a časově náročné.

Z celé literární rešerše je patrné, že existuje celá řada přístupů k hodnocení informačních systémů. I přes značný rozmach tohoto tématu dosud neexistuje žádný přístup, který by snoubil jednoduché a ucelené řešení pro malé i větší firmy. Z tohoto důvodu vznikla tato dizertační práce, která výše uvedené nedostatky pokrývá v navrhované metodice. Metodika vychází ze současné teorie a praxe na základě interview s odborníky. Její ověření bylo provedeno na případových studiích firem různých velikostí. V rámci práce vznikla databáze nedostatků, která shrnuje nejčastější nálezy v oblasti informačních systémů.

4 METODIKA HODNOCENÍ INFORMAČNÍCH SYSTÉMŮ

Kapitola se zaměřuje na inovaci současných přístupů s cílem navrhnout vlastní metodiku pro hodnocení informačních systémů. Postup zpracování je uveden na obrázku č. 26, který prezentuje plán primárního výzkumu, provedení sběru dat a analýzu výsledků. Nejdříve přichází na řadu provedení pilotní studie (kap. 4.1), následují hloubkové rozhovory (kap. 4.2) a vytvoření a testování metodiky (kap. 4.3 a kap. 4.4). Na tomto základě bylo možné metodiku ověřit v praxi (kap. 4.5) a vyhodnotit získané výsledky (kap. 4.6).

Pro splnění cíle a zodpovězení výzkumné otázky byly na základě výsledků pilotní studie a literární rešerše sestaveny a provedeny hloubkové rozhovory, jejichž cílem bylo zjištění nedostatků v oblasti informačních systémů. Po vyhodnocení hloubkových rozhovorů a zjištění hlavních nedostatků byla sestavena metodika pro hodnocení informačních systémů, jako prostředek pro hledání nedostatků v oblasti informačních systémů. Ověření metodiky bylo posléze provedeno pomocí případových studií. V závěrečné fázi bylo možné vyhodnotit celý výzkum a odpovědět na výzkumné otázky.



Obrázek 26: Plán výzkumu, provedení sběru dat a analýza

4.1 Pilotní studie

Cílem pilotní studie bylo zjistit relevanci výzkumného záměru a odhalit chyby v projektovém plánu a v realizovatelnosti výzkumu. Pro vlastní výzkum bylo v rámci pilotního ověření provedeno dotazníkové šetření a konzultace s vybranými respondenty z řad ředitelů informatiky a auditorů informačních systémů. **Účelem pilotní studie bylo ověřit metodický postup dizertační práce.**

Kapitola zabývající se pilotní studií je rozdělena na dvě samostatné podkapitoly. První se detailně zabývá sestavením rámce pro potřeby pilotní studie, který čítá kroky od definice použitých metod až po sestavení otázek pro dotazníkové šetření a interview. Ve druhé části je obsažena podrobná interpretace výsledků pilotní studie.

4.1.1 Sestavení rámce pro potřeby pilotní studie

Postup vytvoření a použití rámce pro potřeby pilotní studie je možné shrnout do několika kroků. V první fázi byly formulovány otázky pro **dotazníkové šetření** a okruhy pro **řízené interview**. Podklady pro vytvoření byly získány z provedené rešerše literatury. Druhá fáze byla zasvěcena sběru dat ať už v dotazníkové formě či ve formě řízených rozhovorů. Následující třetí fáze se zabývala zpracováním výstupu, ve kterém je vyhodnoceno dotazníkové šetření a shrnuty informace z interview. Detailní výstupy z této etapy jsou uvedeny v kapitole 4.1.2.

Otázky dotazníku byly rozděleny do čtyř dimenzí: **podniková úroveň** (např. finanční kritéria), **uživatelská úroveň** (např. spokojenost uživatelů), **procesní úroveň** (např. tok informací mezi procesy) a **strategická úroveň** (např. cíle firmy v oblasti IS/ICT). Každá z těchto dimenzí obsahuje deset oblastí a každá oblast jednu otázku. Celkem bylo v dotazníkovém šetření zahrnuto 40 otázek. Každé otázce bylo přiřazeno 2 až 5 odpovědí a vybrat bylo možné jen právě jednu odpověď.

Podniková dimenze popisuje oblasti spojené s vynaloženými prostředky podniku na IS/ICT. Cílem bylo zjistit, kolik prostředků podnik investuje. Uživatelská dimenze se zabývá spokojeností, podporou a přínosy pro uživatele informačních systémů. Cílem bylo zjistit přínosy, které podnik získává. Provozní dimenze se zabývá tokem informací mezi procesy a správou IS/ICT. Cílem bylo zjistit, jakým způsobem firma informační systém

využívá. Strategická dimenze popisuje dosažení strategie a cílů podniku a pokrytí potřeb firmy. Cílem bylo zjistit, jak by firma mohla informační systém využívat. Detailní popis dimenzí je uveden v tabulce č. 5.

Tabulka 5: Přehled a popis dimenzí použitých v pilotní studii

Dimenze	Podniková Dimenze	Uživatelská dimenze	Provozní dimenze	Strategická dimenze
Zaměření	Podnik	Uživatelé informačního systému	Provoz IS/ICT a firemní procesy	Strategie a cíle firmy
Popis	Oblasti spojené s vynaloženými prostředky podniku na IS/ICT. Cílem je zjistit, kolik prostředků podnik investuje.	Spokojenost, podpora a přínosy pro uživatele informačních systémů. Cílem je zjistit přínosy, které podnik získává.	Tok informací mezi procesy a správa IS/ICT. Cílem je zjistit, jakým způsobem firma informační systém využívá.	Dosažení strategie a cílů podniku, pokrytí potřeb firmy. Cílem je zjistit, jak by firma mohla informační systém využívat.

Rozhovor je na rozdíl od dotazníkového šetření časově náročnější technika pro sběr dat. Minimalizuje se zde na rozdíl od dotazníku neporozumění otázce a zvyšuje se pravděpodobnost, že odpovídá kompetentní osoba. Obsah rozhovoru je vždy přizpůsoben podmínkám zadání a také pracovní pozici a odpovědnostem osoby, se kterou je veden rozhovor. Předpokladem je, že v každé společnosti se uskuteční tolik rozhovorů, aby byly pokryty následující oblasti:

- **organizace a plánování v IT** (rozdělení rolí v IT a směrnice, které se IT týkají, změny v podniku a v podnikové informatice v předchozích letech a plán změn v budoucnu v souvislosti s podnikovou strategií a s vývojem IS/ICT),
- **přístupová oprávnění** (fyzická bezpečnost, informační bezpečnost, ochrana dat, přidělování oprávnění, deaktivace a pravidelná kontrola uživatelských účtů, politika hesel, oddělení pravomocí, úprava kmenových dat, sdílené účty),
- **provoz podnikové informatiky** (zálohování, síťová infrastruktura, Business Continuity Plan, Disaster Recovery Plan, rozhraní mezi aplikacemi, řízení rizik),
- **řízení změn a vývoje** (politika pro evidenci změn, testování a ověřování kvality, rozdělení pravomocí, projektový management).

4.1.2 Interpretace výsledků pilotní studie

Dotazníkové šetření bylo spuštěno na začátku zimního semestru akademického roku 2014/2015. Takto získaná data jsou interpretována v následujících odstavcích. Detailní výsledky pilotní studie jsou zpracovány v příloze č. 2 této práce.

Od září 2014 do ledna 2015 se jej zúčastnilo 63 respondentů z řad menších, středních i větších firem. Většina z těchto společností provozuje své vlastní IT oddělení. Firmy, které výdaje za hardware, software, implementaci a údržbu informatiky sledují, obvykle průměrně za zmíněné vynaloží sumu do 1 procenta vyjádřenou v ročním obratu firmy. Stáří hardwaru se pohybuje v mezích 1-3 roky, starším vybavením disponuje pouze 16 procent firem. Obdobná situace je i u softwaru.

Požadavky zaměstnanců na změny v oblasti IT jsou dle vyjádření zástupců firem brány v úvahu (68 procent). Většina firem využívá školení dodavatele softwaru, ale existují i takové firmy, které školení ke svým softwarovým řešením nedodávají (11 procent). Jen 17 procent dotázaných uvedlo, že jejich systém je velmi intuitivní, přes 65 procent dotázaných má se systémem občasné problémy. Přizpůsobení systému pro pracovní pozici je standardem, přesto 37 procent respondentů uvádí, že některé informace nejsou pro jejich práci důležité. V oblasti nastavení oprávnění se rýsuje z hlediska bezpečnostního incidentu negativní scénář u 15 firem, které mají nastavené v systému u každé pozice stejná oprávnění nebo sdílejí jeden účet. V tom případě pak nelze dohledat, kdo v systému provedl konkrétní změnu. Hledání informací v systému se zdá být velmi snadné pro všechny respondenty. Systémy obvykle nabízí a firmy využívají možnost spolupráce mezi zaměstnanci (46 firem).

70 procent dotázaných tvrdí, že firemní procesy nejsou na zaměstnancích závislé. Zálohování dat vnímá drtivá většina firem jako nutnost, přesto je možné najít i takové firmy, které riziko ztráty dat podstupují. Podklady pro vydání rozhodnutí obvykle pocházejí z informačního systému. Dostupnost i rychlost šíření dat je na dobré úrovni. Informační systém ve 30 procentech podniků je obtížné přizpůsobit novým potřebám firmy. Přes 40 procent respondentů odpovědělo, že funkce systému jsou nadbytečné. Formalizovanou strategií disponuje jen 60 procent podniků, v ostatních případech není strategie dodatečně formalizovaná nebo zcela chybí. V případě IT strategie je situace horší, zpracovanou ji má jen 39 procent dotázaných. Rozšíření systému je snadné jen pro

45 procent respondentů. Přímý ekonomický zisk je možné podle 63 procent podniků docílit nasazením informačního systému. Nepřímé ekonomické přínosy jsou zvažovány u 70 procent firem. Kontrolu IT dělají obvykle lidé, kteří se o podnikovou informatiku starají. 29 procent firem kontroly provádí až v případě problémů.

Výsledky z řízených rozhovorů jsou prezentovány na vzorku osmnácti, převážně výrobních, firem. Ve vzorku byly také firmy zabývající se elektřinou a plynem, administrativou, přepravou a skladováním nebo informačními a komunikačními technologiemi. V roce 2014 a 2015 bylo realizováno 108 interview s lidmi, kteří byli zaměstnanci IT, finančního či controllingového oddělení. Výsledky z těchto interview jsou prezentovány v následujícím odstavci společně se zjištěnými nedostatky. Zahrnuty jsou nálezy z oblasti přístupových oprávnění, provozu podnikové informatiky, řízení změn a řízení vývoje. Do množiny uskutečněných interview byla zahrnuta taková setkání, která splňují následující kritéria: relevantní téma a osoba vzhledem k tématu rozhovoru a délka setkání minimálně 15 minut.

Nejčastějším identifikovaným nedostatkem u zkoumaného vzorku firem byla absence pravidelné kontroly uživatelských účtů, která při pravidelném používání pomáhá zajistit správné přiřazení oprávnění konkrétním uživatelům ve firmě. Při tomto nedostatku se může stát, že zaměstnanec, který změní pracovní pozici a přechází z oddělení do oddělení, může mít v systému více pravomocí, než je k výkonu jeho zaměstnání nutné. Absence kontroly tak může narušit rozdělení pravomocí ve společnosti. Velmi častým problémem je také vypnutí logování u důležitých aplikací, u kterých pak nelze dohledat změny provedené uživateli. Mezi nedostatky také patří chybějící formální postup při zakládání nových uživatelů a blokování odchozích zaměstnanců. V oblasti řízení vývoje a řízení změn je ve zkoumaných společnostech také možné identifikovat některá kritická zjištění. Mezi ně patří zejména neomezený přístup vývojářů do produkčního prostředí. Může tak dojít k situaci, kdy jeden člověk požadovanou (nebo i svou vlastní, nikým nepožadovanou) změnu naprogramuje, otestuje i zavede do produkce. Přidá-li se k předchozímu nedostatku i absence jakékoli kontroly, je poté obtížné dostatečně důvěřovat datům, která jsou v systému uložena. K přehlíženým oblastem v rámci provozu podnikové informatiky či celé společnosti patří Business Continuity a Disaster Recovery. Plány pro obnovení chodu společnosti či IT chybí nebo nesplňují aktuální potřeby společnosti. Problémem může být také nedostatečné monitorování rozhraní mezi aplikacemi.

4.2 Provedení hloubkových rozhovorů

Díky pilotní studii bylo možné ověřit některé postupy a následně identifikovat směr pokračování dizertační práce. Záměr hloubkových rozhovorů vychází z definice výzkumné otázky (kap. 1.2) a jejím cílem je získat podklady pro vytvoření metodiky hodnocení informačních systémů. Kromě pilotní studie (kap. 4.1) patří k podkladům pro sestavení hloubkových rozhovorů kapitola zabývající se použitými metodami (kap. 2) a literární rešerše (kap. 3). Na tuto kapitolu bezprostředně navazuje návrh metodiky pro hodnocení informačních systémů.

Provedení hloubkových rozvorů čítá několik kroků, které jsou postupně rozpracovány v následujících kapitolách. Prvním z nich je sestavení témat rozhovorů (kap. 4.2.1), ve kterém byly dle metodických pokynů vytvořeny otázky pro interview. Po otestování vytvořených témat a zapracování změn (kap. 4.2.2) bylo možné přejít k provedení hloubkových rozhovorů s odborníky z praxe (kap. 4.2.3). V další kapitole (kap. 4.2.4) pak byly všechny výstupy analyzovány, seřízeny a kategorizovány. Na tomto základu vznikla databáze nedostatků a doporučení, která slouží jako podklad pro zodpovězení první výzkumné otázky. Závěrečné vyhodnocení hloubkových rozhovorů (kap. 4.2.5) obsahuje paradigmatický model, který byl vytvořen pomocí otevřeného a axiálního kódování.

4.2.1 Sestavení témat rozhovorů

Pro potřeby hloubkových interview byl použit rozhovor pomocí návodu sestavený na základě pilotní studie a závěrů ze současného stavu vědeckého poznání. V rámci procesu přípravy bylo vytvořeno **15 otevřených otázek** (témat) vztahujících se ke zkušenostem, vnímáním a názorům respondentů. Některé otázky zahrnovaly také podotázky.

Průvodní otázky se zabývají především nedostatky v oblasti informačních systémů, z nich vyplývajících rizik a možných nápravných opatření. Mimo jiné se také věnují kritickým faktorům úspěchu hodnocení, nástrojům, posloupnosti kroků, vyhodnocení a řízení hodnocení informačních systémů. Zabývají se rovněž přínosy a slabými místy hodnocení, jejich častými příčinami nebo odlišnostmi v metodikách. Všechny tematické okruhy jsou uvedeny v příloze č. 2. Primárním cílem hloubkových rozhovorů bylo identifikovat nedostatky v oblasti řízení a provozu informačních systémů a kritéria sloužící pro hodnocení informačních systémů.

4.2.2 Testování témat rozhovorů

Mnoho autorů se shoduje na tom, že fáze testování či předvýzkumu je nezbytná a správný výzkum se bez ní nemůže obejít. Díky testování lze odhalit problémy, které by nastaly v dalších výzkumných fázích.

V rámci testování byla ověřena témata rozhovorů s cílem zjistit, zda v praxi budou fungovat tak, jak bylo zamýšleno. Celkem byl průběh hloubkových rozhovorů testován se **3 respondenty**, přičemž každý z nich zastupoval jednu z níže definovaných skupin (viz kap. 4.2.3). Na základě odhalení několika nedokonalostí bylo možné provést dílčí úpravu formulace otázek.

4.2.3 Provedení hloubkových rozhovorů

Po úspěšném testu na malém vzorku bylo možné dále pokračovat ve výzkumu. Respondenti byli vybráni tak, aby reprezentovali co nejširší skupinu odborníků, kteří mají praktické zkušenosti s hodnocením informačních systémů. Okruh dotazovaných byl vymezen na respondenty, kteří se aktivně:

- podílejí na řízení IT oddělení a mají zkušenosti s interním/externím auditem,
- podílejí na provádění IT auditu (např. členové ISACA, certifikace CISA) nebo
- pracují v oblasti IT Compliance nebo IT Assurance.

Rozhovory byly provedeny s respondenty se zkušenostmi z firem poskytující IT audit (jednalo se zejména o představitele velké čtyřky) či IT Assurance, dále z firem, které mají obsazenou pozici IT Compliance nebo s firmami, jehož IT manažer se aktivně podílí na interním auditu či koordinuje audit externí. Z celého rozhovoru byla pro účely dalšího zpracování pořizována audio nahrávka.

Počet respondentů, jejichž jména nejsou pro účely této práce zveřejněna, byl stanoven na základě kritéria dosažení teoretické nasycenosti dle metodických pokynů. To znamená, že pokud vyhodnocení materiálu a jeho další sběr již nic nového nepřinášejí, je možné výzkum zastavit. V souladu s tímto pravidlem byl rozhovor proveden celkem s **23 odborníky z praxe**. Více rozhovorů nebylo třeba provádět, neboť se ve výstupech opakovaly stejné údaje včetně identických zkušeností.

4.2.4 Kódování

Všechny výstupy z provedených hloubkových rozhovorů byly v této fázi výzkumu analyzovány, seřízeny a kategorizovány. Nejdříve byly podrobeny detailní analýze výstupy týkající se nedostatků v oblasti informačních systémů, z nich vyplývajících rizik a možných nápravných opatření. Jednalo se o velké množství nestrukturovaného materiálu, se kterým bylo nutné dále pracovat. Z tohoto důvodu byla pro zpracování dat vybrána metoda otevřeného kódování. V získaných výstupech byla hledána témata s cílem identifikovat nedostatky v oblasti informačních systémů. Každé významové jednotce byl přiřazen index, který vystihoval zařazení do kategorie. Proces, jehož výstup zachycuje tabulka č. 6, byl opakován v několika iteracích.

Tabulka 6: Rozdělení nedostatků do domén a segmentů

Doména	Index	Segment
Organizace IT oddělení (IT Governance)	G	Politiky a směrnice v oblasti IS/ICT (G1), Řízení IT oddělení (G2 – G4)
Přístupová oprávnění (Access rights)	A	Přidělování a odebírání uživatelských oprávnění (A1 – A5), Pravidelná kontrola uživatelských oprávnění (A6 – A8), Rozdělení pravomocí (A9 – A10), Heslová politika (A11), Administrátorské účty (A12 – A14), Vzdálený přístup (A15)
Změnové řízení (Change management)	C	Proces změnového řízení (C1 – C4), Přístup do produkčního prostředí (C5 – C6)
Provoz IT (IT Operations)	O	Rozhraní mezi aplikacemi (O1), Zálohování (O2 – O3), Plán obnovy v případě provozních problémů (O4 – O6), Fyzická bezpečnost (O7), Logování (O8)

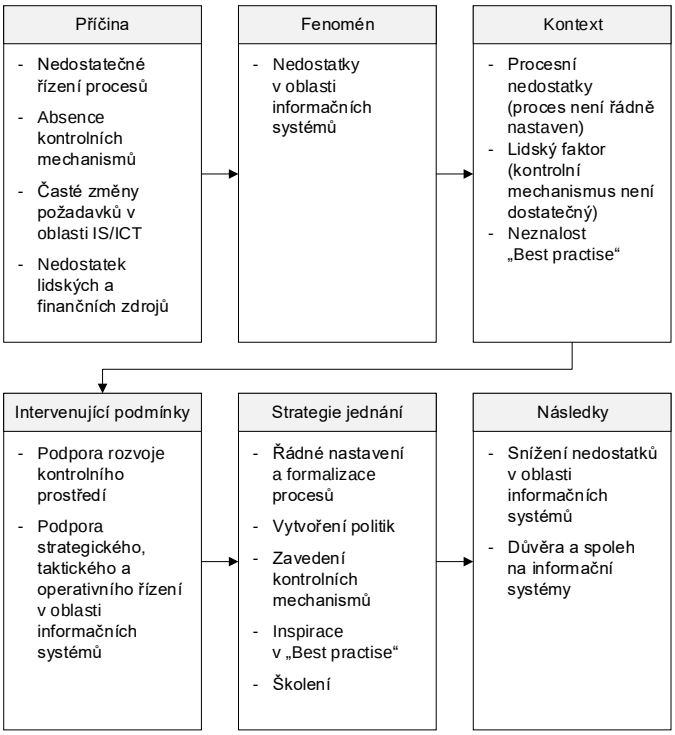
V procesu otevřeného kódování byly definovány **4 hlavní domény** a označeny indexem. Index udává zkratku anglického názvu domény z důvodu snazšího překladu a rozšíření metodiky za hranice České republiky. Doména seskupuje všechny nedostatky s podobným obsahem. V každé doméně je několik segmentů a pod segmenty se skrývá jeden nebo více nedostatků. Označení nedostatků bylo vytvořeno z indexu domény a pořadového čísla nedostatku. U každého nedostatku je definovaný nadpis, index, doména, segment, popis, riziko a doporučení. Zjednodušený seznam nedostatků zobrazuje tabulka č. 7, detailní přehled je uveden v příloze č. 3. Celkem bylo identifikováno **15 segmentů** a **33 nedostatků**.

Tabulka 7: Nedostatky v oblasti informačních systémů

Index	Doména	Segment	Nedostatek
G1	Organizace IT oddělení	Politiky a směrnice v oblasti IS/ICT	IT politiky nejsou formálně dokumentovány, schváleny a publikovány.
G2	Organizace IT oddělení	Řízení IT oddělení	Podnik nemá ucelenou strategii vedení a správy společnosti.
G3	Organizace IT oddělení	Řízení IT oddělení	Nedostatečné řízení rizik v oblasti IS/ICT.
G4	Organizace IT oddělení	Řízení IT oddělení	IT oddělení není řízeno centrálně a nezodpovídá za některé IT oblasti.
A1	Přístupová oprávnění	Přidělování a odebírání uživatelských oprávnění	V produkčním systému je aktivní a užívaný účet, který není schválený.
A2	Přístupová oprávnění	Přidělování a odebírání uživatelských oprávnění	Proces udělování a odebírání přístupových oprávnění není řádně nastaven.
A3	Přístupová oprávnění	Přidělování a odebírání uživatelských oprávnění	Žádosti o přidělení přístupových oprávnění nejsou řádně zdokumentovány.
A4	Přístupová oprávnění	Přidělování a odebírání uživatelských oprávnění	V produkčním systému je aktivní a užívaný účet zaměstnance, který již ve společnosti nepracuje.
A5	Přístupová oprávnění	Přidělování a odebírání uživatelských oprávnění	Uživatelské účty nejsou odebrány včas.
A6	Přístupová oprávnění	Pravidelná kontrola uživatelských oprávnění	Není prováděna periodická kontrola přístupových oprávnění.
A7	Přístupová oprávnění	Pravidelná kontrola uživatelských oprávnění	Periodická kontrola přístupových oprávnění není formalizovaná.
A8	Přístupová oprávnění	Pravidelná kontrola uživatelských oprávnění	Periodická kontrola přístupových oprávnění není dostatečná.
A9	Přístupová oprávnění	Rozdělení pravomocí	Uživatelé mají přístup k citlivým transakcím.
A10	Přístupová oprávnění	Rozdělení pravomocí	Není zpracována matice neslučitelných oprávnění.
A11	Přístupová oprávnění	Heslová politika	Nedostatečné nastavení heslové politiky.
A12	Přístupová oprávnění	Administrátorské účty	Sdílený administrátorský účet.

A13	Přístupová oprávnění	Administrátorské účty	Uživatelé s neomezeným oprávněním.
A14	Přístupová oprávnění	Administrátorské účty	Nedostatečné monitorování aktivit privilegovaných účtů.
A15	Přístupová oprávnění	Vzdálený přístup	Vzdálený přístup do produkčního systému není monitorován.
C1	Změnové řízení	Proces změnového řízení	Proces změnového řízení není řádně nastaven.
C2	Změnové řízení	Proces změnového řízení	Změna není testovaná před implementací do produkčního prostředí.
C3	Změnové řízení	Proces změnového řízení	Nedostatečné rozdělení pravomocí v oblasti změnového řízení.
C4	Změnové řízení	Proces změnového řízení	Testovací prostředí není vytvořeno, změny jsou implementovány přímo do produkce.
C5	Změnové řízení	Přístup do produkčního prostředí	Neomezený přístup interních vývojářů do produkčního prostředí.
C6	Změnové řízení	Přístup do produkčního prostředí	Neomezený přístup dodavatele do produkčního prostředí.
O1	Provoz IT	Rozhraní mezi aplikacemi	Nedostatečné monitorování rozhraní mezi aplikacemi.
O2	Provoz IT	Zálohování	Proces zálohování dat je nedostatečný.
O3	Provoz IT	Zálohování	Nedostatečné testování záloh.
O4	Provoz IT	Plán obnovy v případě provozních problémů	Zastaralá infrastruktura.
O5	Provoz IT	Plán obnovy v případě provozních problémů	Není implementován havarijní plán a plán kontinuity obchodních činností.
O6	Provoz IT	Plán obnovy v případě provozních problémů	Havarijní plán a plán kontinuity nepokrývají všechna rizika.
O7	Provoz IT	Fyzická bezpečnost	Fyzická bezpečnost serverovny.
O8	Provoz IT	Logování	Vypnuté logování produkční databáze.

Příčinami vzniku nedostatků v oblasti informačních systémů se zabývá analýza vedoucí na **vytvoření paradigmatického modelu**. Na základě otevřeného kódování byla využita metoda axiálního kódování, která představuje vyšší úroveň analýzy dat. Při axiálním kódováním byly identifikovány vazby mezi kategoriemi, které byly následně uspořádány do schématu, jehož detailní popis uvádí obrázek č. 27.



Obrázek 27: Paradigmatický model nedostatků v oblasti informačních systémů

Jako hlavní příčiny vzniku nedostatků v oblasti informačních systémů byly v rámci hloubkových rozhovorů identifikovány oblasti jako nedostatečné řízení procesů, absence kontrolních mechanismů, časté změny požadavků v oblasti IS/ICT nebo nedostatek lidských a finančních zdrojů. Vznik nedostatků je obvykle zapříčiněn nedostatečným nastavením některých procesů, lidským faktorem nebo neznalostí či ignorací „Best practise“. Mezi podmínky pro snížení počtu nedostatků se řadí podpora rozvoje kontrolního prostředí a podpora strategického, taktického a operativního řízení v oblasti informačních systémů. Mezi cílené a záměrné aktivity, které vedou k eliminaci nedostatků, patří řádné nastavení a formalizace procesů, vytvoření politik, zavedení kontrolních mechanismů, inspirace v „Best practise“ a školení zaměstnanců. Očekávaným výsledkem je snížení nedostatků v oblasti informačních systémů a z toho pramenící důvěra a spoleh na informační systémy.

4.2.5 Vyhodnocení hloubkových rozhovorů

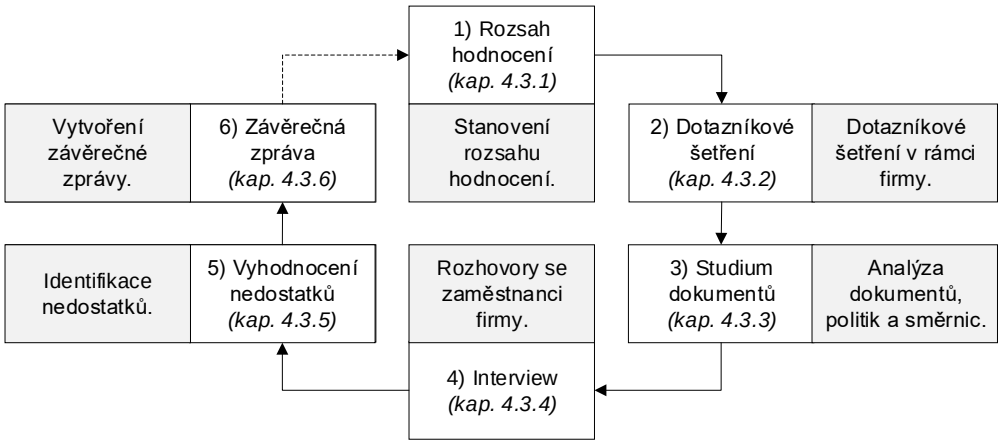
Hloubkový rozhovor byl zvolen jako základní metoda pro provedení primárního výzkumu. Bylo připraveno 15 otevřených témat vztahujících se ke zkušenostem, vnímáním a názorům respondentů. Průvodní otázky se zabývají především nedostatky v oblasti informačních systémů, z nich vyplývajících rizik a možných nápravných opatření. Po úspěšném testu na malém vzorku byly provedeny rozhovory s 23 respondenty z praxe v souladu s pravidlem teoretická saturace. Pro vyhodnocení byla použita transkripce údajů, jejich přepis z poznámek a audionahrávek a následně otevřené a axiální kódování.

V procesu otevřeného kódování byly údaje roztřízeny na dílčí celky a poté definovány čtyři hlavní domény, které seskupují všechny nedostatky s podobným obsahem. V každé doméně je několik segmentů a pod segmenty se skrývá jeden nebo více nedostatků. Nedostatky byly řádně pojmenovány, třízeny a klasifikovány. U každého nedostatku byl definovaný mimo jiné jeho detailní popis, riziko a doporučení. Celkem bylo identifikováno **33 hlavních nedostatků v oblasti provozu a řízení informačních systémů a možných opatření vedoucích k jejich odstranění**. Výsledek z této fáze výzkumu vede na zodpovězení výzkumné otázky dizertační práce (VO1). Databáze nedostatků dále posloužila v další fázi výzkumu, která se zabývá vytvořením metodiky pro hodnocení informačních systémů. Kromě sestavení metodiky byla použita i v procesu vyhodnocení informačních systémů. Detailní popis vytvoření metodiky a zapojení výsledků z této fáze výzkumu uvádí kapitola 4.3.

V rámci této části výzkumu vznikl také paradigmatický model, který hledal příčiny vzniku a odstranění nedostatků v oblasti informačních systémů. Mezi hlavní příčiny se řadí nedostatečné řízení procesů, absence kontrolních mechanismů, časté změny požadavků v oblasti IS/ICT nebo nedostatek lidských a finančních zdrojů. Jako hlavní aktivity, které vedou k eliminaci nedostatků, patří řádné nastavení a formalizace procesů, vytvoření politik, zavedení kontrolních mechanismů, inspirace v „Best practise“ a školení zaměstnanců.

4.3 Vytvoření metodiky hodnocení informačních systémů

Svět IS/ICT je v současné době mimo jiné formován požadavky z mnoha oblastí zahrnující normy, zákony, standardy či statutární nebo jiné formy auditu. Metodika, jejíž navržení je cílem této práce, ale není šita na míru přímo konkrétním standardům či normám, nýbrž se snaží identifikovat hlavní nedostatky v oblasti provozu a řízení informačních systémů a možných opatření vedoucích k jejich odstranění nezávisle na konkrétním výkladu regulatorních požadavků. Na základě vyjádření expertů, kteří se zabývají IT auditem, řízením podnikové informatiky či souladem a ujištěním v oblasti IS/ICT, lze konstatovat, že nedostatky se často opakují nezávisle na implementaci informačních systémů nebo regulatorních požadavcích. Z tohoto důvodu je metodika navržena jako obecná a použitelná ve firmách, které spadají pod různá omezení či regulaci v oblasti IS/ICT. Cílem metodiky je provést hodnocení ve velmi krátkém čase a odhalit podstatné nedostatky identifikované experty v této oblasti. Očekávaným výsledkem je snížení nedostatků v oblasti informačních systémů a z toho pramenící důvěra a spoleh na informační systémy.



Obrázek 28: Fáze metodiky hodnocení informačních systémů

Průběh hodnocení je možné shrnout do šesti po sobě jdoucích fází uvedených na obrázku č. 28. První představuje stanovení rozsahu hodnocení (kap. 4.3.1), ve kterém jsou definovány hodnocené systémy a časové období. Následuje dotazníkové šetření (kap. 4.3.2), studium dokumentů (kap. 4.3.3) a interview (kap. 4.3.4). Všechny tři zmíněné se v souladu s databází nedostatků zaměřují na prověření systému vývoje a údržby, posouzení IS/ICT politik, norem a pokynů týkajících se bezpečnosti IS/ICT, informační

ochrany, řízení IT projektů a kontrolu zabezpečení před neoprávněným přístupem. Použitím těchto metod roste míra ujištění, že získané informace jsou kompletní a přesné. Dotazník představuje velmi rychlou metodu pro zjištění předběžného stavu informačního systému. Na něj navazuje studium dokumentů, které pečlivě ověřuje odpovědi uvedené v dotazníku. Finálním krokem ověření je interview, které čítá jak předpřipravené otázky vyplývající z metodiky, tak otázky vzešlé z dosavadního průběhu hodnocení. Vyhodnocení je předmětem páté fáze (kap. 4.3.5), ve které dochází k posouzení získaných výsledků a identifikaci nedostatků v oblasti provozu a řízení informačních systémů. Poslední fáze hodnocení se zabývá závěrečnou zprávou (kap. 4.3.6). V tomto kroku je nutné vytvořit report obsahující nedostatky a opatření vedoucí k jejich odstranění a odsouhlasit získané výsledky s představiteli firmy. Závěrečná zpráva obsahuje návrh účinných řešení, úspor a provozních zlepšení.

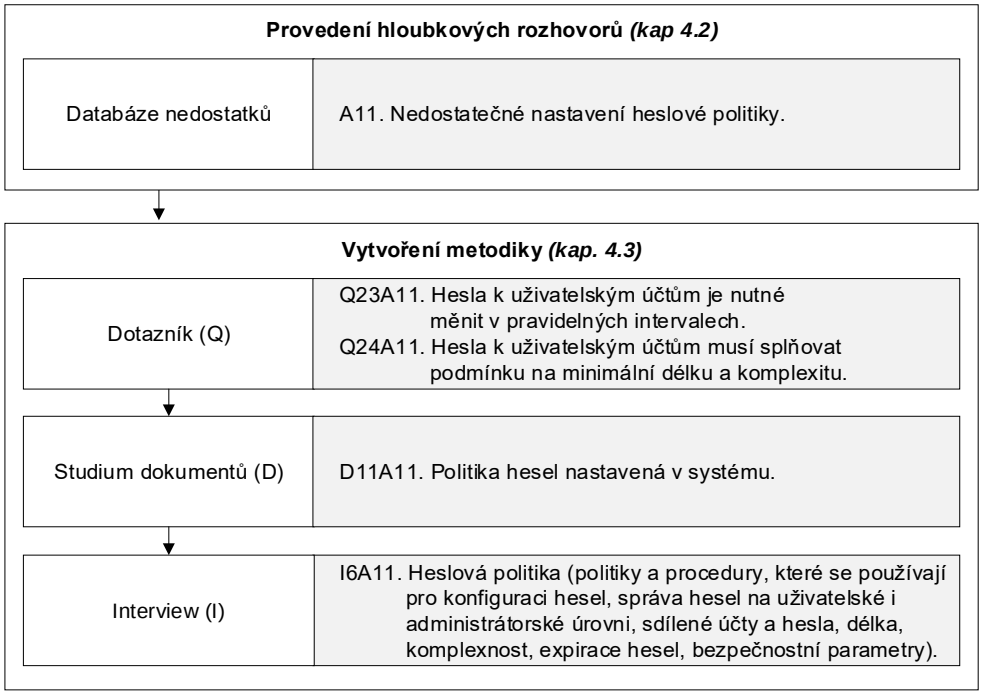
4.3.1 Rozsah hodnocení

První fáze metodiky hodnocení informačních systémů v sobě zahrnuje dotazník obsahující **identifikační otázky** a **přehled hodnocených systémů**. Rozsah hodnocení je předmětem dohody zadavatele hodnocení (např. management firmy nebo IT oddělení) a hodnotící strany (konzultanta). Nezbytné je také určit sledované období.

Identifikační otázky byly sestaveny pro získání řídicích a identifikačních parametrů, dle kterých bude možné provést analýzu týkající se velikosti firmy, oboru podnikání, vlastnických poměrů či velikosti IT oddělení. Jejich přehled je uveden v příloze č. 4 pod označením P1 – P5. Jedná se o uzavřené otázky s možností jedné odpovědi. Po vyplnění identifikačních otázek je nutné definovat, jaké aplikace, operační systémy a databáze budou předmětem hodnocení. Podklad pro vypracování přehledu hodnocených systémů je zahrnutý v příloze č. 4 pod označením S. Pokud je v rozsahu hodnocení více aplikací, operačních systémů nebo databází, je nutné tomu přizpůsobit dotazníkové šetření (kap. 4.3.2), studium dokumentů (kap. 4.3.3) i interview (kap. 4.3.4). Vše je detailně popsáno v příslušných kapitolách. Metodika může sloužit nejen pro informativní účely vedení firmy, ale i jako příprava na audit. V takovém případě je výhodné zvolit v rozsahu hodnocení stejné systémy jako budou definovány v připravovaném auditu. V případě, že je dohodnuto provést hodnocení více systémů, je vhodné ještě před začátkem hodnocení porozumět, jaké procesy systémy pokrývají a jak jsou vzájemně propojené.

4.3.2 Dotazníkové šetření

Dotazník byl v dizertační práci vytvořen na základě analýzy výsledků hloubkových rozhovorů a literární rešerše. Je použit jako jedna z metod v navrhované metodice, jejímž cílem je odhalit nedostatky v oblasti informačních systémů. Postup vytvoření otázek, který je patrný z obrázku č. 29, je popsán v následujících řádcích. Východiskem pro zpracování otázky byl vždy identifikovaný a kategorizovaný nedostatek. Pro názorný příklad byl vybrán z databáze nedostatků nedostatek A11, který se týká nedostatečného nastavení heslové politiky. Pro potřeby dotazníku byly v souladu s tímto tématem vytvořeny dvě otázky: Q23A11 a Q24A11. Jak může být patrné, každé otázce byly přiřazeny: unikátní index, který se skládá z písmena Q *(Questionnaire)* označující dotazník, pořadové číslo otázky (v tomto případě 23 a 24) a odkaz na databázi nedostatků (v tomto případě A11). Stejný postup byl aplikován pro všech 33 nedostatků. Dohromady bylo tímto způsobem zpracováno **50 otázek**.



Obrázek 29: Postup vytvoření otázek

V případě, že je v rozsahu hodnocení kromě aplikace zahrnuta i databáze a operační systém, případně více systémů, je nutné vyplnění dotazníku tomuto faktu přizpůsobit. Otázky kategorie QG z oblasti řízení IT oddělení je postačující vyplnit pouze jednou, otázky z ostatních domén je nutné pro každý systém vyplnit odděleně.

V dotazníku byly použity trichotomické otázky s možností odpovědi: *Ano*, *Ne* či *Částečně*. Otázky byly postaveny tak, aby odpověď *Ano* indikovala správné nastavení systému a odpovědi *Ne* nebo *Částečně* naznačovaly nedostatek. Respondent má také možnost uvést krátký komentář. Celý dotazník je uveden v příloze č. 4 této práce. Otázky jsou rozděleny podle domén: organizace IT oddělení čítá otázky Q1 – Q7, přístupová oprávnění Q8 – 30, řízení změn Q31 – Q40 a provoz IT následně Q41 – Q50.

4.3.3 Studium dokumentů

Na základě databáze nedostatků byl sestaven seznam dokumentů, které je vhodné při hodnocení prozkoumat podrobněji. Postup vytvoření seznamu je možné také ilustrovat pomocí obrázku č. 29. Na nedostatek A11, který byl vybraný pro vzorový příklad, navazuje dokument označený indexem D11A11 týkající se politiky hesel nastavené v systému. V metodice je každý nedostatek, otázka i dokument označen unikátním indexem. Při hodnocení se lze pak odkázat přímo na číslo dokumentu. Písmeno D *(Documents)* označuje studium dokumentů, následuje pořadové číslo dokumentu (v tomto případě 11) a poté je uveden nezbytný odkaz na nedostatek v databázi nedostatků (v tomto případě A11). Dokumenty byly rozděleny dle domény na organizaci IT oddělení (D1 – D4), přístupová oprávnění (D5 – D13), řízení změn (D14 – D16) a provoz IT (D17 – D20). Celkem bylo takto identifikováno **20 dokumentů**. Jejich přehled obsahuje příloha č. 4 této práce.

Cílem studia dokumentů je zpřesnit výsledky dotazníkového šetření. Spíše než o vnější analýzu, která se zabývá kontextem vzniku, se jedná o vnitřní analýzu, která se věnuje přímo obsahu dokumentu. Prvním stupněm hodnocení je zjištění, že dokument existuje. Pokud ano, je následně nezbytné zpřesnit odpověď z dotazníku a potvrdit či vyvrátit nedostatek z něj plynoucí. U směrnic či politik je možné v rámci hodnocení zjistit, kdy byly dokumenty naposledy aktualizovány, kdo k nim má přístup a jak probíhá jejich distribuce a aktualizace. U některých nedostatků nebyl vytvořený žádný požadavek na dokument, u jiných byl vytvořen požadavek na více dokumentů. Například pro nedostatek týkající se aktivních účtů odchozích zaměstnanců (A5) je nutné obdržet seznam aktivních uživatelů v systému (D6A5) a seznam odchozích zaměstnanců (D7A5). Porovnáním těchto dokumentů je možné nedostatek A5 potvrdit či vyvrátit. V případě hodnocení více systémů je nutné vyžádat pro každý systém odděleně dokumenty týkající se domén: přístupová oprávnění (DA), změnové řízení (DC) a provoz IT (DO).

4.3.4 Interview

Závěrečné ověření výsledků z dotazníku a studia dokumentů přináší interview. Přestože je rozhovor na rozdíl od dotazníkového šetření a studia dokumentů časově náročnější technika pro sběr dat, minimalizuje se zde možnost neporozumění otázce a zvyšuje se pravděpodobnost, že odpovídá kompetentní osoba. V rámci navrhované metodiky hodnocení informačních systémů byl použitý rozhovor pomocí návodu. Návod byl sestaven na základě domén a kategorií vzešlých z hloubkových rozhovorů s odborníky z praxe a následným uspořádáním oblastí do vhodného pořadí.

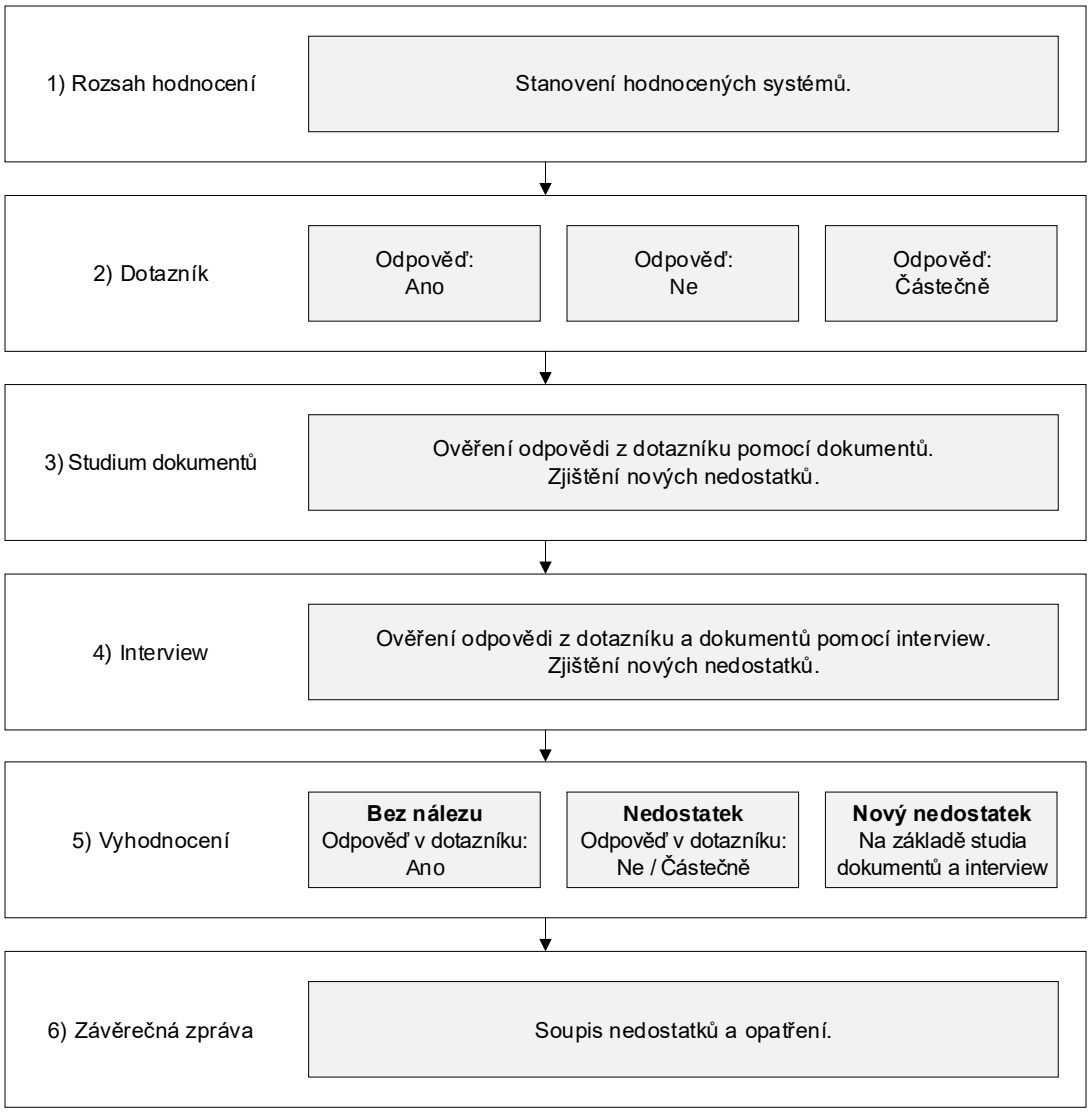
Obsah rozhovoru musí být vždy přizpůsoben rozsahu hodnocení, pracovní pozici a odpovědnostem osoby, se kterou je veden rozhovor. Předpokladem je, že v každé společnosti se uskuteční tolik rozhovorů, aby byly pokryty všechny oblasti metodiky v rámci rozhovorů.

Na rozdíl od dotazníku a studia dokumentů, byl seznam témat pro interview sestaven na základě 15 segmentů, které vznikly v rámci fáze kódování (kap. 4.2.4). Jedno téma tedy na rozdíl od dotazníku může vést na více nedostatků. Pro vzorový nedostatek A11 bylo vytvořeno téma zabývající se problematikou heslové politiky s označením I6A11. Písmeno I *(Interview)* označuje rozhovor, následuje pořadové číslo tématu (v tomto případě 6) a nechybí odkaz na databázi nedostatků (A11). Jiným příkladem mohou být nedostatky G2, G3 a G4, které byly v rámci kódování zahrnuty pod jeden segment. V rámci interview je tedy pro tyto nedostatky vytvořeno jen jedno společné téma.

Témata rozhovoru byly stejně jako otázky v dotazníku a u studia dokumentů rozděleny dle domény na organizaci IT oddělení (I1 – I2), přístupová oprávnění (I3 – I8), řízení změn (I9 – I10), a provoz IT následně (I11 – I15). Celkem bylo tímto způsobem identifikováno **15 témat**. Jejich přehled obsahuje příloha č. 4 této práce. Kromě předpřipravených témat, které vznikly v rámci metodiky, je možné pokládat i otázky vyplývající z průběhu hodnocení. Cílem je zpřesnit výsledek z dotazníku a potvrdit či vyvrátit nedostatek. V případě hodnocení více systémů je stejně jako u dotazníkového šetření a u studia dokumentů nutné projít témata zabývající se přístupovými oprávněními (IA), změnovým řízením (IC) a provozem IT (IO) pro každý systém odděleně.

4.3.5 Vyhodnocení nedostatků

Cílem vyhodnocení, které probíhá na základě analýzy výsledků základních kamenů metodiky (dotazníku, studia dokumentů a interview), je získat přehled o stavu IS/ICT ve sledované firmě. Jelikož jsou zde kombinovány kvantitativní i kvalitativní přístupy, bylo nutné pro tento účel aplikovat vyhodnocení pomocí smíšené strategie. Cílem bylo získat na položené otázky spolehlivější a relevantnější odpovědi. Pro vyhodnocení bylo z fázových modelů vybráno sekvenční kombinování typu QUAN → qual, které se dle Hendla (2016, s. 295) používá v případě, že výsledky jednoho přístupu (dotazník) jsou podstatné pro uplatnění dalšího přístupu (studium dokumentů a interview).



Obrázek 30: Postup vyhodnocení nedostatků

Kvantitativní přístup v podobě dotazníku (QUAN) je nadřazený a kvalitativní přístupy (qual) zahrnující studium dokumentů a interview jsou podřazené a slouží jen pro ověření. Kvantitativní přístup je použitý pro zkoumání vychýlených nebo neočekávaných výsledků. Z výše uvedeného je patrné, že je jako základ použita kvantitativní metoda a kvalitativní přístup se použije pouze pro vyjasnění některých oblastí.

Postup vyhodnocení nedostatků v rámci metodiky hodnocení informačních systémů, který ilustruje obrázek č. 30, je popsán v následujících řádcích. V první fázi je nutné stanovit hodnocené systémy, sledované období a odpovědět na identifikační otázky. Identifikační otázky lze rozšířit pro potřeby specifického výzkumu. Další krok představuje vyplnění dotazníku představitelem hodnocené firmy. Dle rozdělení pravomocí může celý dotazník vyplnit jedna čí více osob. Otázky jsou položeny tak, aby odpověď *Ano* indikovala, že je vše v pořádku, a naopak odpovědi *Ne* a *Částečně* naznačovaly nedostatek. Díky tomu jsou už v této fázi k dispozici předběžné výsledky, k jejichž zpřesnění dochází pomocí studia dokumentů a interview. Ověřují se zde pomocí podpůrných dokumentů a definovaných témat rozhovorů, zda dotazníková odpověď odpovídá realitě. Na základě tohoto zpřesnění je nedostatek potvrzen či vyvrácen. Jednoznačné a jasné značení otázek a nedostatků v databázi nedostatků pomáhá k rychlé navigaci mezi jednotlivými dokumenty metodiky. Díky tomu je pak možné velmi snadno zjistit, která otázka, dokument či téma vede na jaký nedostatek.

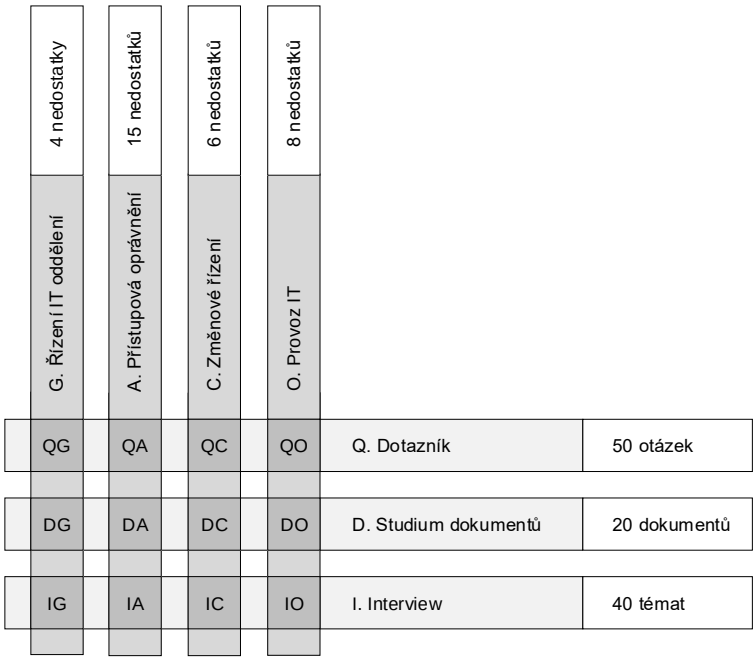
Pomocí dotazníku je možné nalézt jen předdefinované nedostatky, naproti tomu ve fázi studia dokumentů a interview je možné nalézt úplně nové nedostatky. V takovém případě je nejdříve nutné zvážit, zda se jedná o relevantní nedostatek. Pro vyhodnocení mohou pomoci například nové normy, regulace či zákony v oblasti IS/ICT, osvědčené přístupy „Best practise“ nebo hloubkové rozhovory mezi odborníky v praxi. Podobný postup lze využít i v případě podezření, že některý nedostatek či doporučení již není v souladu s aktuálními přístupy.

V případě přidání nového nedostatku do databáze nedostatků je třeba postupovat podle následujícího návodu. Do databáze nedostatků je třeba přidat doménu, segment, název, popis, riziko a doporučení, které se k nedostatku vztahuje. Dle metodiky sestavení otázek (obrázek č. 29) je dále nutné vytvořit otázky do dotazníku (kap. 4.3.2), definovat příbuzné dokumenty (kap. 4.3.3) a témata rozhovoru (kap. 4.3.4).

4.3.6 Závěrečná zpráva

Díky postupu, který byl definován v předchozí kapitole, je možné identifikovat nedostatky v oblasti provozu a řízení informačních systémů. Fáze závěrečná zpráva na ni zcela navazuje a přidává několik, převážně formálních, kroků.

Prvním z nich je příprava formalizované závěrečné zprávy, jejímž obsahem je minimálně informace o stanoveném rozsahu, hodnocených systémech, časovém omezení, termínu provedení hodnocení a přehledu nedostatků. Každá část metodiky přímo navazuje na konkrétní nedostatek uvedený v databázi, která představuje hlavní podklad pro vypracování přehledu nálezů. Návaznost metodiky s databází nedostatků je uvedena na obrázku č. 31. Pro účely vytvoření závěrečné zprávy je možné upravit formulaci popisu, rizika nebo doporučení tak, aby byl nález co nejpřesněji charakterizován.



Obrázek 31: Matice provázanosti metodiky s databází nedostatků

Druhým, neméně podstatným krokem, je představení nedostatků na společné schůzce s představiteli firmy. Benefitem pro společnost je, že obdrží v jednoduché formě přehled o stavu provozu a řízení informačních systémů včetně popisu nedostatků, rizik i doporučení. Metodika hodnocení je v souladu s Demingovým cyklem PDCA (viz obrázek č. 28), což znamená, že lze hodnocení po zapracování opatření opakovat a výsledky poté srovnat.

4.4 Testování metodiky

Ještě před ověřením v praxi byla metodika hodnocení informačních systémů testována v souladu s druhou výzkumnou otázkou pomocí případové studie na dvou konkrétních firmách. Předmětem testování byla zejména časová náročnost, porozumění otázek a vyhodnocení nedostatků. V rámci testování bylo v metodice provedeno několik drobných úprav týkajících se formulací otázek v dotazníku, formulace požadavků na dokumenty a formulace témat v interview. Pro přehlednost byly všechny nedostatky v databázi nedostatků, otázky v dotazníku, dokumenty i témata interview označeny indexem.

Časová náročnost metodiky, která je uvedena v tabulce č. 8, byla rozdělena do dvou kategorií. Časová náročnost pro klienta představuje čas, který musí zaměstnanec nebo zaměstnanci firmy vynaložit pro účely hodnocení. Časová náročnost hodnocení shrnuje čas strávený hodnocením informačního systému a vyhodnocením nedostatků. Dle závěrů testování je časová náročnost pro klienta 5–10 hodin a náročnost hodnocení 10–20 hodin. Náročnost může růst na straně klienta v případě, že některé dokumenty jsou částečně nedostupné nebo nejsou jasně definovány odpovědnosti za některé procesy. Na straně hodnocení může časová náročnost růst s rozšířením rozsahu hodnocení.

Tabulka 8: Časová náročnost hodnocení informačních systémů pro jeden systém

Pořadí	Fáze	Časová náročnost klienta	Časová náročnost hodnocení
1	Rozsah hodnocení	1 hod. Společná schůzka	1 hod. Společná schůzka
2	Dotazníkové šetření	0,5–1 hod. Vyplnění dotazníku	1 hod. Předběžné vyhodnocení nedostatků
3	Studium dokumentů	1–3 hod Příprava dokumentů	3–8 hod. Ověření odpovědí
4	Interview	1-3 hod. Společná schůzka	1–3 hod. Společná schůzka, ověření odpovědí
5	Vyhodnocení	1 hod. Konzultace	1–3 hod. Vyhodnocení nedostatků
6	Závěrečná zpráva	0,5–1 hod. Společná schůzka	2–4 hod. Příprava závěrečné zprávy, společná schůzka
	Celkem	**5–10 hodin**	**10–20 hodin**

4.5 Ověření metodiky v praxi

Pro ověření v praxi byla v rámci této dizertační práce použita mnohonásobná případová studie popisující aplikaci metodiky hodnocení informačních systémů v kategorii malých, středních a velkých firem. Jedná se o kvalitativní ověření, jelikož metodika je založena na smíšeném přístupu a vyhodnocení je prováděno pomocí metodologické triangulace. Cílem kapitoly je odpovědět na druhou výzkumnou otázku.

Postup ověření metodiky čítá několik po sobě jdoucích kroků, které jsou v souladu s druhou výzkumnou otázkou zaměřující se na identifikaci nedostatků v provozu a řízení informačních systémů při použití metodiky v praxi (kap. 1.2). Nejdříve byly pro účely ověření vybrány tři případy (kap. 4.5.1), kterým jsou později věnovány samostatné kapitoly (kap. 4.5.2 – 4.5.4). Každý případ byl nejdříve analyzován samostatně a poté došlo ke srovnání všech případů mezi sebou (kap. 4.5.5). Na tomto základě došlo ke třízení a abstrakci. V práci byla použita komparativní struktura pro vyhodnocování případové studie, která obsahuje části, které postupně rozebírají jednotlivé případy.

4.5.1 Výběr případů

Podmínky výběru případů byly stanoveny v souladu s druhou výzkumnou otázkou na základě klasifikace podniků dle databáze Bureau van Dijk (2017a a 2017b) následně:

- malý podnik (provozní výnosy do 1 milionu euro, celková aktiva do 2 milionů euro a počet zaměstnanců nepřevyšuje 15),
- střední podnik (provozní výnosy v rozmezí 1–10 milionů euro, celková aktiva v rozmezí 2–20 miliony euro a počet zaměstnanců v intervalu 15–150),
- velký podnik (provozní výnosy vyšší nebo rovny 10 milionů euro, celková aktiva vyšší nebo rovny 20 milionů euro a počet zaměstnanců převyšuje 150).

Na základě těchto kritérií byly zvoleny pro výzkum tři firmy, které působí na území České republiky. Převažující obor podnikání je dle členění Českého statistického úřadu (2017) postupně: profesní, vědecké a technické činnosti, informační a komunikační činnosti a zpracovatelský průmysl. Jména firem nejsou pro účely této práce zveřejněna.

4.5.2 Případová studie v kategorii malých firem

Pro případovou studii v oblasti malých firem byla zvolena společnost se 14 zaměstnanci zabývající se pořádáním reklamních akcí, mediálních kampaní a výstavnictvím. Vnitřní strukturu společnosti tvoří obchodní a ekonomické oddělení, výroba, produkce a grafické DTP studio. Správu podnikové informatiky zajišťuje jeden externí spolupracovník. Případová studie postupuje dle fází navržené metodiky hodnocení informačních systémů. V rámci rozsahu hodnocení stanoveném ve spolupráci s jednatelem firmy bylo zvoleno hodnocené období na celý kalendářní rok 2016 a hodnocená aplikace jako Money S4.

Po stanovení rozsahu hodnocení proběhla fáze dotazníkového šetření, ve které byl vyplněn dotazník IT specialistou ve spolupráci s jednatelem firmy. Z 50 otázek, které obsahuje celý dotazník, bylo kladně zodpovězeno 29 otázek, záporně 18 otázek a 3 otázky s odpovědí částečně. Po přiřazení odpovědí k jednotlivým nedostatkům do vyhodnocovacího reportu, který je dostupný v příloze č. 5 této práce, bylo možné identifikovat celkem 16 nedostatků ve všech čtyřech doménách metodiky. V oblasti organizace IT oddělení to jsou nedostatky zaměřené na IT strategii (G1) a řízení rizik (G3). Oblast přístupových oprávnění indikuje nedostatky v pravidelné kontrole uživatelských účtů (A6, A7, A8), matici neslučitelných oprávnění (A10) a administrátorských účtech (A14). Až na dvě výjimky jsou negativní odpovědi také v oblasti změnového řízení (C1, C2, C3 a C4). V oblasti provozu byly identifikované předběžné nedostatky týkající se přenosu dat mezi aplikacemi (O1) a plánů obnovy v případě provozních problémů (O5 a O6).

Třetí fáze metodiky se zabývá detailním studiem dokumentů. Na základě požadavků definovaných v metodice byly dodány všechny dokumenty, které byly ve firmě k dispozici. Po jejich prostudování byly zjištěny další potenciální nedostatky. První se týká oblasti procesu udělování a odebírání uživatelských účtů (A2). Přestože je ve firmě zavedena formální politika, neexistují důkazy týkající se změn uživatelských oprávnění. Druhý nedostatek byl identifikován v oblasti odebírání uživatelských účtů (A5) na základě porovnání aktivních uživatelů v systému se seznamem aktuálních zaměstnanců. V systému byl nalezen aktivní uživatelský účet zaměstnance, který ve firmě již nepracuje. Potvrzeny byly oblasti týkající se IT strategie (strategie není aktualizovaná) a administrátorských účtů (aktivity privilegovaných účtů nejsou sledovány). Dále nebyly dodány podklady pro oblast řízení rizik, pravidelné kontroly uživatelských účtů, matice

neslučitelných oprávnění, změnového řízení, rozhraní mezi aplikacemi a plánů obnovy v případě provozních problémů.

V rámci interview byla diskutována postupně všechna témata definovaná v metodice. Otázky na řízení IT oddělení byly směřovány na jednatele firmy a ostatní otázky na IT specialistu. Po zjištění, že většina nedostatků pramení z oblasti změnového řízení, byla velká pozornost věnována právě tomuto tématu. Na základě interview bylo potvrzeno, že v aplikaci Money S3 hodnocená firma neprovádí žádné změny programového kódu. Změny distribuuje pouze dodavatel řešení v rámci pravidelných aktualizací. Na základě dohody s jednatelem firmy byla celá doména změnového řízení vyjmuta z hodnocení a počet nedostatků tak mírně klesl. Stejný postup byl aplikován i v oblasti rozhraní mezi aplikacemi, jelikož systém žádným nedisponuje. Všechny další nedostatky, které vzešly z přechozích fází, byly potvrzeny.

V rámci vyhodnocení bylo identifikováno 11 nedostatků, se kterými bylo dále pracováno. Jelikož spolu některé úzce souvisí, byl ve zprávě uveden jen jeden zástupce. Celkem se tak do závěrečné zprávy dostalo **8 nedostatků**, které popisovaly možná rizika i doporučená opatření. Po ukončení hodnocení informačního systému byla uspořádána schůzka s jednateli firmy s cílem prezentovat a objasnit zjištěné nedostatky a doporučení. Představitelé firmy akceptovali všechny předložené nedostatky a dohodli se na dalším pokračování. V oblastech G1, A2, A5, A6 a O5 hodlají provést nápravná opatření dle doporučení a u G3, A10, A14 budou pouze akceptována vyplývající rizika.

Tabulka 9: Přehled nedostatků zjištěných v případové studii v kategorii malých firem

Doména	Nedostatek
Organizace IT oddělení	IT politiky nejsou formálně dokumentovány, schváleny a publikovány (G1). Nedostatečné řízení rizik v oblasti IS/ICT (G3).
Přístupová oprávnění	Proces udělování a odebírání přístupových oprávnění není řádně nastaven (A2). Uživatelské účty nejsou odebrány včas (A5). Není prováděna periodická kontrola přístupových oprávnění (A6). Není zpracována matice neslučitelných oprávnění (A10). Nedostatečné monitorování aktivit privilegovaných účtů (A14).
Změnové řízení	Změnové řízení není prováděno v aplikaci definované v rozsahu hodnocení.
Provoz IT	Není implementován havarijní plán a plán kontinuity obchodních činností (O5).

4.5.3 Případová studie v kategorii středních firem

Předmětem druhé případové studie z kategorie středních firem je společnost zabývající se poskytování IT služeb a vývojem software. Firma nabízí služby v oblasti poskytování internetu a IPTV. Celkem firma zaměstnává 38 pracovníků, z toho 15 se aktivně podílí na vývoji a správě systému, který byl předmětem hodnocení. Hodnocené období bylo stanoveno na celý rok 2016.

Dotazník byl vyplněn ředitelem firmy s následujícím vyhodnocením. Kladně bylo zodpovězeno 47 otázek a záporně 3 otázky. Po přiřazení odpovědí k jednotlivým nedostatkům do vyhodnocovacího reportu, který je uveden v příloze č. 5, byly předběžně identifikovány 3 nedostatky v oblasti periodické kontroly uživatelských oprávnění (A8), přístupu vývojářů do produkčního prostředí (C5) a plánů obnovy v případě provozních problémů (O5). V rámci studia dokumentů byly výše zmíněné nedostatky potvrzeny, a navíc identifikovány dva nové. První byl zjištěn pomocí porovnání nově příchozích zaměstnanců s novými účty v systému. Pro testovací účely mimo schvalovací proces si jeden ze zaměstnanců založil nový účet. Druhý nedostatek byl zjištěn na základě analýzy dokumentu, který se týká provedených změn v systému. Některé změny nebyly před implementací testovány.

Pomocí interview pak bylo všech **5 zjištěných nedostatků** potvrzeno a v rámci vyhodnocení zapracováno do závěrečné zprávy. První nedostatek se týkal aktivního a užívaného účtu, který nebyl formálně schválený. Pomocí těchto účtů mohou být provedeny neoprávněné operace nebo změny finančních údajů. Společnosti bylo v tomto případě doporučeno formalizovat správu přístupových práv. Druhý nedostatek byl zaměřen na oblast pravidelné kontroly uživatelských oprávnění. Společnost prováděla pouze periodickou kontrolu uživatelských účtů, která nezahrnovala kontrolu uživatelských oprávnění. Pravidelné kontroly přístupových práv jsou obvykle prováděny, aby uživatelé měli dostatečný přístup k výkonu svých pracovních povinností. Bez pravidelné kontroly přístupových práv mohou mít uživatelé více oprávnění, než je požadováno (např. situace, kdy byl zaměstnanec převeden z jednoho oddělení do druhého), což vede k potenciálnímu riziku úmyslné a nezjistitelné manipulace s finančními údaji. Pro eliminaci tohoto rizika je nutné kontrolovat oprávnění v systému pro každého uživatele. Třetí nedostatek se týkal testování nových funkcionalit před implementací do

produkčního prostředí. Bylo totiž zjištěno, že některé změny nebyly před implementací testovány. Bez správných testovacích postupů existuje riziko selhání systému, které může způsobit finanční ztráty, nepřístupnost nebo ztrátu finančních údajů. Nedostatky v zálohovacích postupech, které zjištěny nebyly, zvyšují toto riziko. V tomto případě je doporučováno před implementací do produkčního prostředí testovat jakékoli změny. Čtvrtý nedostatek byl nalezen také v oblasti změnového řízení. Vývojáři měli neomezený přístup do produkčního prostředí. Je zde vysoké riziko implementace neotestovaných nebo neoprávněných změn do produkčního prostředí, které mohou mít vliv na konzistenci dat a funkčnost systému. Pro snížení rizika je nezbytné vypnout nebo zablokovat účty vývojářů v produkčním prostředí. Pro nouzové případy by měl být použit havarijní účet, k němuž by měl být přístup omezen a udělen formálně, pouze v odůvodněných případech a po nezbytnou dobu. V oblasti provozu IT byl identifikován pátý nedostatek týkající se havarijního plánu a plánu kontinuity obchodních činností. Společnost neměla formalizován havarijní plán DRP *(Disaster Recovery Plan)* ani plán kontinuity obchodních činností BCP (Business Continuity Plan), které by jí umožnili efektivně řídit kontinuitu činností v oblasti financí a dalších podpůrných procesů. Jejich absence může vést ke zpoždění při obnově kritických obchodních procesů a systémů. Pro eliminaci tohoto rizika je nutné oba plány řádně formalizovat, pravidelně aktualizovat a testovat.

Management firmy byl v závěru hodnocení seznámen s výsledky. Nedostatky A1, A8, C2 a O5 považují za důležité a počítají s jejich nápravou. Rizika vzešlá z nedostatku C5 hodlají z důvodu omezených kapacit akceptovat.

Tabulka 10: Přehled nedostatků zjištěných v případové studii v kategorii středních firem

Doména	Nedostatek
Organizace IT oddělení	Bez nálezu.
Přístupová oprávnění	V produkčním systému je aktivní a užívaný účet, který není schválený (A1). Periodická kontrola přístupových oprávnění není dostatečná (A8).
Změnové řízení	Změna není testovaná před implementací do produkčního prostředí (C2). Neomezený přístup interních vývojářů do produkčního prostředí (C5).
Provoz IT	Není implementován havarijní plán a plán kontinuity obchodních činností (O5).

4.5.4 Případová studie v kategorii velkých firem

Předmětem třetí případové studie, tentokráte z kategorie velkých firem, je potravinářská společnost, která se specializuje na výrobu nealkoholických nápojů. Celkem firma zaměstnává 750 pracovníků, IT oddělení má 8 zaměstnanců. Společně s IT ředitelem firmy byl stanoven hodnocený systém SAP R3 a hodnocené období jako kalendářní rok 2016.

Z 50 otázek, které zodpověděl IT manažer společnosti, bylo 48 odpovězeno kladně a jen dvě záporně. Po přiřazení odpovědí k jednotlivým nedostatkům do vyhodnocovacího reportu, který je uveden v příloze č. 5, byly předběžně identifikovány 2 nedostatky. Jednalo se o matici neslučitelných oprávnění (A10) a o rozdělení pravomocí v oblasti změnového řízení (C3). V rámci studia dokumentů byly nedostatky dále rozšířeny. Porovnáním aktivních účtů v systému se seznamem odchozích pracovníků, bylo zjištěno, že někteří z nich mají stále aktivní účet (A5). Po odchodu z firmy se ale naštěstí do systému nepřihlásili. Další nedostatek vychází z nedostatečného testování záloh (O3). Testování záloh nebylo prováděno ani v rámci ověřování DRP plánu. Pomocí interview byly nedostatky dále prověřovány, žádné nové ale zjištěny nebyly. Bylo pouze potvrzeno, že ve více případech došlo k naprogramování, otestování a migraci změny do produkce jednou osobou. Dále nebyla ve společnosti zavedena matice neslučitelných oprávnění, kdy hrozí riziko neoprávněného přístupu, zneužití informací či zpronevěry.

V rámci vyhodnocení, které je uvedeno v příloze č. 5 této práce, byly **identifikovány 4 nedostatky**. První z nich se zabývá deaktivací uživatelských účtů. Ačkoli by měl být všem zaměstnancům po ukončení jejich pracovního poměru zamezen přístup do systému, byly v systému účty odchozích pracovníků stále aktivní. Neblokováním či nesmazáním přístupových účtů bývalým zaměstnancům v nejkratší možné době se zvyšuje riziko nepovoleného přístupu k aplikaci a k citlivým datům, které může vést k úmyslné změně dat či jejich smazání. To může vést až k nedůvěryhodnosti finančních dat. K incidentu obvykle dochází zejména kvůli nedostatku komunikace vůči IT oddělení. V tomto případě by bylo vhodné zvážit posílení mechanismů, které zajistí včasný přenos informací o potřebě zablokování nebo smazání účtů. Druhý nedostatek byl identifikován v oblasti rozdělení pravomocí. V rámci informačního systému nebyla zpracována matice neslučitelných oprávnění. Z tohoto důvodu zde hrozí riziko neoprávněného přístupu, zneužití informací či zpronevěry. Společnosti bylo doporučeno zpracovat matici

neslučitelných oprávnění pro informační systém a zavést automatickou kontrolu čtyř očí pro rizikové operace (např. změna čísla bankovního účtu dodavatele a odběratele). V oblasti změnového řízení byl objeven třetí nedostatek. V průběhu hodnocení bylo identifikováno nedostatečné oddělení povinností v procesu vývoje a testování nových vylepšení. V jednom nebo více případech došlo k naprogramování, otestování a migraci změny do produkce jednou osobou. Oddělení pravomocí v rámci procesu řízení změn snižuje riziko provedení změny, která nebyla řádně testována a autorizována, což může vést k poškození dat nebo k poškození funkčnosti programu. V případě tohoto nálezu je doporučováno, aby změny prováděl jiný zaměstnanec než vývojář. Může to být správce systému, který nemůže změnit kód programu. Další variantou může být provedení změn prostřednictvím instalačních balíčků, které by byly implementovány do testovacího prostředí a po provedení testů by se stejný balíček instaloval do produkčního prostředí. Řešením by mohlo být také zavedení kontroly, v níž by operace jako vložení nebo úprava dat v klíčových tabulkách byly prověřeny odpovědnými pracovníky. Čtvrtý nedostatek se týká testování záloh. V průběhu hodnocení bylo zjištěno, že i když má společnost formalizovaný DRP plán, není součástí jeho testování zpětná kontrola záloh. Rizikem je, že v případě nouze může společnost ztratit všechna produkční data. Společnost by proto měla zvážit ověřování záloh v rámci testování DRP plánu.

V závěrečné fázi byl management firmy seznámen s výsledky. Všechny zjištěné nedostatky A5, A10, C3 a O3 považuje za důležité a plánuje nastavit procesy a kontroly dle předložených doporučení.

Tabulka 11: Přehled nedostatků zjištěných v případové studii v kategorii velkých firem

Doména	Nedostatek
Organizace IT oddělení	Bez nálezu.
Přístupová oprávnění	Uživatelské účty nejsou odebrány včas (A5). Není zpracována matice neslučitelných oprávnění (A10).
Změnové řízení	Nedostatečné rozdělení pravomocí v oblasti změnového řízení (C3).
Provoz IT	Nedostatečné testování záloh (O3).

4.5.5 Vyhodnocení případových studií

Cílem případových studií bylo v souladu s druhou výzkumnou otázkou formulovanou v úvodu práce ověřit metodiku hodnocení informačních systémů v praxi. Za tímto účelem byly zpracovány tři případové studie, které se postupně detailně věnují hodnocení informačního systému v malé, střední a velké společnosti. Plán provedení mnohonásobných případových studií zahrnoval definici plánu výzkumu (zvolení konkrétní malé, střední a velké firmy, použití metodiky hodnocení informačních systémů a definice výzkumné otázky), přípravu a sběr dat (identifikace a potvrzení nedostatků) a analýzu a závěry (identifikace alternativních interpretací a zobecnění studovaných případů).

V rámci předběžné identifikace pomocí dotazníkového šetření bylo odhaleno celkem 19 nedostatků ve všech třech zmíněných případech. Díky ověření pomocí studia dokumentů a interview bylo zjištěno, že na jednom hodnoceném systému neprobíhá změnové řízení a po dohodě s představitelem firmy nebyla tato doména vůbec hodnocena. Počet potenciálních nedostatků tak klesl na 15. V následném zpřesňování výsledků byly potvrzeny všechny nedostatky vyplývající z dotazníkového šetření, a navíc identifikovány ještě další. Počet nedostatků se zvýšil v tuto chvíli na 20. Jelikož spolu ale některé úzce souvisí, bylo rozhodnuto, že ve výsledné zprávě bude uveden jen jeden zástupce. **Celkem tak bylo ve třech společnostech identifikováno 14 jedinečných nedostatků**, které jsou přehledně uvedeny v tabulce č. 12. Nejvíce nedostatků bylo nalezeno v oblasti přístupových oprávnění, nejméně pak v oblastech řízení IT oddělení a provozu IT. Nedostatky týkající se odebírání uživatelských oprávnění, chybějících plánů pro obnovu obchodních činností a matice neslučitelných oprávnění byly nalezeny ve více případech. Časová náročnost hodnocení byla průměrně 2 až 3 dny.

Největší rozdíly mezi jednotlivými případy dobře vykresluje doména řízení IT oddělení. Zatímco u malé společnosti byla zjištěna nízká formalizace politik a procesů, u střední a velké nebyl identifikován nález žádný. Mála firma vůbec inkasovala nejvíce nedostatků. Pro studovanou společnost však výsledky slouží spíše pro zjištění současného stavu. Obecně je cílem představitele firmy seznámit s riziky, o kterých mnohdy nevěděli. Naopak zde popisovaná střední a velká společnost splňuje podmínky statutárního auditu a každý zjištěný nedostatek může z pohledu auditu snižovat věrohodnost dat v systému a zvyšovat jeho náročnost. Pokud však firma provede nápravná opatření dle doporučených

postupů v metodice, dokáže zvýšit věrohodnost dat v systému a ušetřit finanční prostředky. Některé nedostatky lze odstranit snadno (např. doplnit periodickou kontrolu uživatelských oprávnění), jiné jsou náročnější (např. změna procesu změnového řízení). Každý nedostatek byl prezentován představitelům firem na závěr každého hodnocení. Po detailním vysvětlení všech rizik a doporučení všichni představitelé firem s nedostatky souhlasili a hodlají až na výjimky podpořit jejich odstranění V několika případech obvykle z kapacitních či finančních důvodů hodlají pouze akceptovat riziko.

Tabulka 12: Souhrnný přehled nedostatků zjištěných v případových studiích

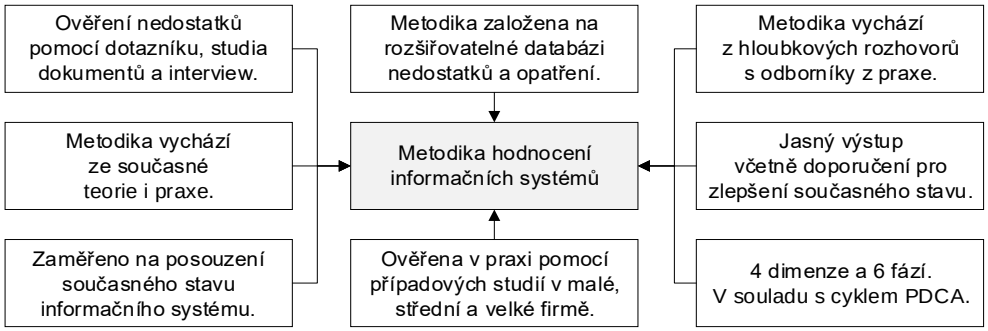
Index	Nedostatek	Malá společnost	Střední společnost	Velká společnost
G1	IT politiky nejsou formálně dokumentovány, schváleny a publikovány.	Nedostatek 1 (malá spol.)	Bez nálezu	Bez nálezu
G3	Nedostatečné řízení rizik v oblasti IS/ICT.	Nedostatek 2 (malá spol.)	Bez nálezu	Bez nálezu
A1	V produkčním systému je aktivní a užívaný účet, který není schválený.	Bez nálezu	Nedostatek 1 (střední spol.)	Bez nálezu
A2	Proces udělování a odebírání přístupových oprávnění není řádně nastaven.	Nedostatek 3 (malá spol.)	Bez nálezu	Bez nálezu
A5	Uživatelské účty nejsou odebrány včas.	Nedostatek 4 (malá spol.)	Bez nálezu	Nedostatek 1 (velká spol.)
A6	Není prováděna periodická kontrola přístupových oprávnění.	Nedostatek 5 (malá spol.)	Bez nálezu	Bez nálezu
A8	Periodická kontrola přístupových oprávnění není dostatečná.	Bez nálezu	Nedostatek 2 (střední spol.)	Bez nálezu
A10	Není zpracována matice neslučitelných oprávnění.	Nedostatek 6 (malá spol.)	Bez nálezu	Nedostatek 2 (velká spol.)
A14	Nedostatečné monitorování aktivit privilegovaných účtů.	Nedostatek 7 (malá spol.)	Bez nálezu	Bez nálezu
C2	Změna není testovaná před implementací do produkčního prostředí.	Nehodnoceno	Nedostatek 3 (střední spol.)	Bez nálezu
C3	Nedostatečné rozdělení pravomocí v oblasti změnového řízení.	Nehodnoceno	Bez nálezu	Nedostatek 3 (střední spol.)
C5	Neomezený přístup interních vývojářů do produkčního prostředí.	Nehodnoceno	Nedostatek 4 (střední spol.)	Bez nálezu
O3	Nedostatečné testování záloh.	Bez nálezu	Bez nálezu	Nedostatek 4 (velká spol.)
O5	Není implementován havarijní plán a plán kontinuity obchodních činností.	Nedostatek 8 (malá spol.)	Nedostatek 5 (střední spol.)	Bez nálezu

4.6 Vyhodnocení stanoveného cíle a zodpovězení výzkumných otázek

Kapitola sumarizuje výsledky výzkumu dizertační práce ve dvou částech. První podkapitola je zaměřena na vyhodnocení stanoveného cíle a druhá podkapitola zodpovídá výzkumné otázky. Jedná se pouze o přehledné shrnutí zahrnující odkazy na kapitoly a přílohy, které obsahují detailní rozpracování konkrétní problematiky.

4.6.1 Vyhodnocení stanoveného cíle

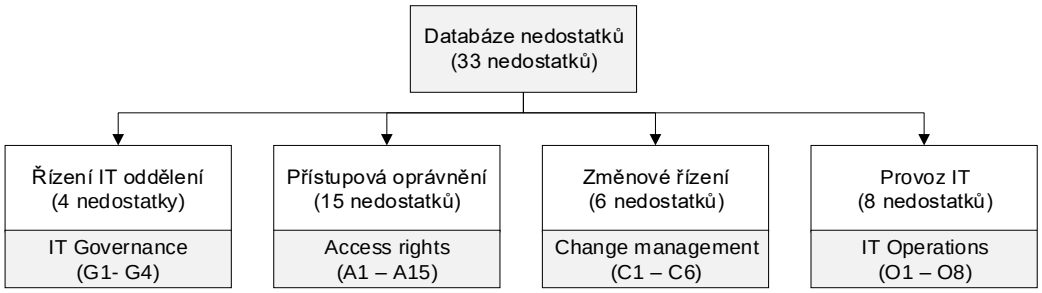
Cílem dizertační práce bylo **navržení vlastní metodiky pro hodnocení informačních systémů**. Jako východiska pro zpracování metodiky sloužily zejména závěry k současnému stavu vědeckého poznání (kap. 3), pilotní studie (4.1) a výsledky hloubkových rozhovorů (kap. 4.2). Metodika vznikla na základě identifikovaných a kategorizovaných nedostatků dle navrženého postupu v této práci (obrázek č. 29). Průběh hodnocení je možné shrnout do šesti po sobě jdoucích fází. První představuje stanovení rozsahu hodnocení, ve kterém jsou definovány hodnocené systémy a časové období. Následuje dotazníkové šetření, studium dokumentů a interview. Použitím těchto metod roste míra ujištění, že získané informace jsou kompletní a přesné. Vyhodnocení je předmětem páté fáze, ve které dochází k posouzení získaných výsledků a identifikaci nedostatků v oblasti provozu a řízení informačních systémů. Poslední fáze hodnocení se zabývá závěrečnou zprávou, která obsahuje návrh účinných řešení, úspor a provozních zlepšení. Cílem metodiky je provést hodnocení ve velmi krátkém čase a odhalit podstatné nedostatky identifikované experty v této problematice. Očekávaným výsledkem je snížení nedostatků v oblasti informačních systémů a z toho pramenící důvěra a spoleh na informační systémy. Detailní popis všech zmíněných fází a podkladů pro metodiku hodnocení informačních systémů je uveden v kapitole 4.3 a příloze č. 4.



Obrázek 32: Specifikace navržené metodiky hodnocení informačních systémů

4.6.2 Zodpovězení výzkumných otázek

V rámci dizertační práce byly na základě současného stavu vědeckého poznání a požadavků z praxe stanoveny dvě výzkumné otázky (kap. 1.2). **První výzkumná otázka** byla zaměřena na nalezení hlavních nedostatků v oblasti provozu a řízení informačních systémů a možných opatření vedoucích k jejich odstranění. Pro zodpovězení této otázky byly provedeny hloubkové rozhovory s odborníky z praxe a na tomto základu vytvořena databáze nedostatků a opatření (kap. 4.2), která slouží jako základní kámen nové metodiky hodnocení informačních systémů. Nedostatky byly řádně pojmenovány, třízeny a klasifikovány do 4 domén a 15 segmentů. Systematickou koncepci třídění databáze nedostatků přináší grafika na obrázku č. 33. U každého nedostatku byl definován mimo jiné jeho detailní popis, riziko a doporučení. Celkem bylo identifikováno 33 hlavních nedostatků v oblasti provozu a řízení informačních systémů a možných opatření vedoucích k jejich odstranění. Více informací a detailní zpracování postupu výzkumu je zpracováno v kapitole 4.2 a přílohách č. 2 a 3 této práce.



Obrázek 33: Struktura databáze nedostatků

V souladu s cílem práce a první výzkumnou otázkou byla stanovena **druhá výzkumná otázka** zaměřující se na použití vytvořené metodiky hodnocení informačních systémů v praxi. Byl využit přístup mnohonásobné případové studie pro výzkum v kategorii malých, středních a velkých firem. Každý případ byl nejdříve analyzován zvlášť a poté došlo ke srovnání všech případů mezi sebou. Souhrnná zpráva obsahuje zprávy o jednotlivých případech a celkové zhodnocení včetně komparace a končí vřazením zkoumaného případu do širších souvislostí. Celkem bylo ve třech společnostech identifikováno 14 jedinečných nedostatků. Všechny identifikované nedostatky byly představeny zástupcům zkoumaných firem, kteří je následně beze zbytku akceptovali. Průběh případových studií a podrobné výsledky shrnuje kapitola 4.5 a příloha č. 5.

4.7 Diskuze a omezení

Následující text se věnuje zhodnocení vlastního výzkumu a jeho zasazení do širších souvislostí. V rámci vyhodnocení jsou diskutovány hlavní otázky dosažených výsledků z mnoha hledisek. Dále se diskutují příležitosti a omezení navržené metodiky. Současně byly vytipovány hlavní oblasti praktického využití celého výzkumu.

Výzkum je pro informační disciplíny a profese velmi podstatný. Bez něho by základna akademických znalostí stagnovala a pokrok v praxi by byl mnohem obtížnější. Nové technologické a ekonomické faktory, které zasahují z velké části i do hodnocení informačních systémů, proměňují informační prostředí mnoha komplexními způsoby. Hodnocení informačních systémů je disciplína, která integruje znalosti z různých oborů čítající především informační a komunikační technologie, finance a řízení podniků, projektů a bezpečnosti. Jde o náročnou disciplínu, u které roste význam z mnoha důvodů. Informační a komunikační technologie jsou nezbytné vzhledem ke globalizaci a zvyšující se dynamice trhů, zkracování inovačních cyklů, zvyšování intenzity konkurenčního boje, dynamiky a komplexnosti vnitropodnikových procesů a rozhodování. Zasahují do všech oblastí managementu a týkají se stále většího okruhu zainteresovaných osob. Právě globalizace vede ke standardizaci informačních systémů, které poskytují platformu pro všechny ostatní odvětví podniku. Bez zavedení pravidelných kontrol není možné dosáhnout kvality v celosvětovém měřítku. Společnosti v současnosti čelí také výzvám v podobě rostoucí komplexity způsobu řízení informací. K tomu přispívá zejména množství a roztříštěnost informačních systémů, intenzivní zadávání manuálních dat a v neposlední řadě i pozůstatky mnoha fúzí a akvizic mezi podniky. Zvyšují se tak rizika v oblasti podvodů kvůli rostoucímu počtu operací i díky tlaku regulátorů na vyšší transparentnost. Poskytování všech údajů totiž znamená nejen vyšší náklady, ale představuje i vyšší riziko jejich zneužití. Důvody pro zavedení hodnocení informačních systémů vedoucí k eliminaci nedostatků tak dnes stojí na pevných základech.

Téma dizertační práce úzce navazuje na řízení a ekonomiku podniku. Hodnocení informačního systému a identifikace nedostatků se totiž promítá jak do řízení (např. nedostatky související s rozdělením pravomocí a organizací IT oddělení), tak i do ekonomiky podniku (např. negativní dopad ryzích IT nedostatků do oblasti výroby či financí, nedostatky

související se zpronevěrou, nízká efektivita statutárního auditu v případě disfunkčního IT prostředí nebo poskytnutí negativního výroku SOX s dopadem na cenu akcií na burze). Mezi výhody navržené metodiky patří zejména získání přehledu o aktuálním stavu IS/ICT a identifikace hlavních nedostatků a návrhů opatření. Díky výsledkům hodnocení podnik získá cenné informace pro manažerské rozhodování (např. nedostatky související s IT strategií či organizací IT oddělení) nebo na jejich základě dokáže realizovat konkurenční výhodu (např. formulováním plánů kontinuity obchodních činností). Metodika ve svých doporučeních podporuje **řádné nastavení a formalizaci procesů** (např. proces změn přístupových oprávnění), **vytvoření politik** (např. migrace změn do produkčního prostředí) či **zavedení kontrolních mechanismů** (např. monitorování aktivit privilegovaných účtů). Argumentem pro hodnocení informačních systémů pomocí navrhované metodiky je i hledisko auditu, který je možné zvládnout efektivněji a s vyšší mírou úspěšnosti. Soulad IS/ICT s regulačními požadavky se pak může stát běžnou praxí při řízení organizace. Pravidelným hodnocením může být také dosažena vyšší kvalita IT služeb, které vedou ke komplexnosti podnikových aktivit. Díky výsledkům metodiky je také možné předvídat negativní skutečnosti, připravit se na ně a odvrátit tak případné hrozby. K dalším výhodám metodiky patří možnost zařazení více systémů do hodnocení jedné společnosti.

Ačkoli význam hodnocení může být pro firmy různých velikostí odlišný, základní přínosy zůstávají stejné. V **malé firmě** je cílem seznámit představitele firmy s riziky, o kterých mnohdy nemají tušení. Obvykle tyto firmy nesplňují podmínky statutárního auditu, jehož součástí může být i IT audit, a hodnocení informačních systémů u nich neprobíhá vůbec nebo jen velmi zřídka. Naopak **střední a velké společnosti** obvykle splňují podmínky statutárního auditu nebo musí být dokonce v souladu se zákonem SOX. Poté každý zjištěný nedostatek externího hodnotitele může v tomto případě snižovat věrohodnost dat v systému a zvyšovat finanční i časovou náročnost hodnocení. Pokud ale firma provede nápravná opatření dle doporučených postupů definovaných v předkládané metodice, dokáže zvýšit věrohodnost dat v systému a ušetřit finanční prostředky.

Mezi příležitosti výzkumu lze připsat jeho rozšíření za hranice České republiky. Hloubkové rozhovory, ze kterých vznikl seznam nedostatků a na základě kterých byla sestavena metodika hodnocení, byly provedeny pouze s respondenty z České republiky. Stejně tak firmy, na kterých byla metodika ověřena, byly české. V této souvislosti by bylo

velmi zajímavé ověřit výzkum i s lidmi z jiných zemí a ověřit metodiku na jiných firmách. Na tomto základě byly v rámci dalšího výzkumu, který již není součástí této práce, provedeny hloubkové rozhovory přes audio konferenci s experty ze střední a východní Evropy, USA a Číny dle stanovených podmínek v kapitole 4.2.3. Na základě předběžných výsledků lze konstatovat, že databáze nedostatků i metodika je použitelná i v jiných částech světa. Během rozhovorů nebyly identifikovány dramatické odchylky či nalezeny zcela nové informace. Použitím metodiky mimo oblast naší republiky bylo dopředu plánováno a nahrávají tomu například názvy domén, které byly přeloženy do angličtiny včetně jejich zkratek. K dalším příležitostem patří také studium závislostí. Masivním používáním metodiky a získáním více výsledků může být současný výzkum rozšířen o studium závislostí jednotlivých nedostatků pomocí klasifikačního stromu.

Proces řízení organizací není jednoduchou činností a spolu s rozvojem IS/ICT jsou patrné některé dopady na řízení firmy. Zároveň je stále velkou výzvou eliminace slabých míst a hrozeb, které se kvůli vývoji v této oblasti mohou v průběhu času měnit. Zmíněný fakt může být pro navrženou metodiku považován jako hrozba. Databáze nedostatků je vytvořena na základě interview s odborníky, kteří se pohybují v současné praxi. Pokud se ale změní významným způsobem IS/ICT prostředí, bude nutné metodiku aktualizovat. V souladu s tímto předpokladem je metodika nachystána a jako její součást jsou definovány postupy pro přidávání položek do databáze nedostatků.

Současným omezením i výhodou zároveň je fakt, že metodika není přizpůsobena na míru konkrétnímu informačního systému. Jako praktický příklad lze uvést kontrolu administrátorských účtů. V případě hodnocení informačním systému SAP je všeobecně platné, že administrátorským účtům jsou přiřazeny profily SAP_ALL a SAP_NEW. V jiných informačních systémech ale platí jiné názvosloví či zcela jiné pojetí administrátorských účtů. Ještě před hodnocením je proto třeba informační systém teoreticky nastudovat a v jeho průběhu korektně definovat administrátorský účet. Může se jednat například o roli v systému, která umožnuje vytvářet nové uživatele a měnit oprávnění. Rizika všech nedostatků je nutné vždy řádně zvážit. Například při nálezu aktivního účtu bývalého zaměstnance v systému nelze jednoznačně říci, že riziko je vysoké. Po analýze času posledního přihlášení a oprávnění účtu lze riziko výrazně snížit či zvýšit a dospět tak k přesnějším závěrům.

5 PŘÍNOSY DIZERTAČNÍ PRÁCE

Kapitola shrnuje přínosy dizertační práce, které významným způsobem obohacují současné vědecké poznání a praktickou i pedagogickou oblast. Přínosy pro praxi zahrnují vymezení samotné metodiky, zmapování aktuálních poznatků a identifikaci možností pro další výzkum. Přínos pro praxi představuje především využití metodiky a získání výsledků vedoucích k eliminaci nedostatků v oblasti informačních systémů. Výsledky dizertační práce lze také využít pro pedagogickou praxi. Uvedené přínosy jsou detailně rozebrány v následujících podkapitolách.

5.1 Přínosy pro vědecké poznání

Přestože téma dizertační práce, které bylo v rámci rešerše podpořeno 126 odkazy na odbornou literaturu, je velmi aktuální, neexistuje dosud žádný přístup, který by snoubil jednoduché a ucelené řešení pro malé i větší firmy. Ze studia současného stavu vědeckého poznání vyplynulo, že převládají nedostatky v oblasti zaměření metodik pouze na určité spektrum firem, procesů či systémů. Nejednoznačné se jeví výsledky, doporučení i finanční a časová náročnost. Z tohoto důvodu vznikla tato dizertační práce, která výše uvedené nedostatky pokrývá v navrhované metodice. Dizertační práce vychází z výzkumné činnosti Ústavu informatiky na Fakultě podnikatelské VUT v Brně a průběžné publikační aktivity. Hodnocení informačního systému a identifikace nedostatků úzce souvisí s řízením i ekonomikou podniku. V oblasti dalšího výzkumu je možné rozšířit metodiku za hranice České republiky nebo po získání více výsledků analyzovat závislosti nedostatků pomocí rozhodovacích stromů. Práce přispěla k rozšíření vědeckého poznání především k:

- identifikaci vědeckých metod vhodných pro použití v dané problematice,
- detailním shrnutí a komparativním porovnání současných přístupů k hodnocení informačních systémů na základě studia současné světové i české literatury,
- vytvoření vědecké metodiky pro oblast hodnocení informačních systémů,
- propojení požadavků z praxe s vědeckými a výzkumnými postupy,
- definování paradigmatického modelu pro oblast příčin vzniku nedostatků, na jehož základě je možné lépe pochopit kontext, podmínky, následky i řešení nedostatků ve firemním prostředí.

5.2 Přínosy pro praxi

Metodika hodnocení informačních systémů vychází ze současného stavu vědeckého poznání a požadavků z praxe. Byla vytvořena na základě interview s odborníky a její ověření bylo provedeno pomocí případových studiích. V rámci práce vznikla databáze nedostatků, která shrnuje nejčastější nálezy v oblasti informačních systémů. Cílem metodiky je provést hodnocení ve velmi krátkém čase a odhalit podstatné nedostatky identifikované experty v této oblasti. Očekávaným výsledkem je snížení nedostatků ve firemním prostředí a z toho pramenící důvěra a spoleh na IS/ICT. Přínos pro praxi je zaměřený zejména na použití metodiky ve firemním prostředí a na návrhy opatření v rámci procesů spojených s informačními systémy. Díky konkrétním návrhům opatření, které metodika poskytuje, je možné zajistit vyšší úroveň zabezpečení a minimalizovat tak rizika spojená se ztrátou způsobenou ať již havárií systému nebo také chybami pracovníků, případně jejich jednáním v rozporu se zákonem. Díky stanovení politik a formalizaci procesů je možné minimalizovat zneužití prostředků zaměstnavatele v rozporu se zájmy organizace. Přínosy pro praxi je možné shrnout do v následujících oblastí:

- vytvoření metodiky pro posuzování informačních systémů ve firemním prostředí,
- metodika podporuje řádné nastavení a formalizaci procesů, vytvoření politik a zavedení kontrolních mechanismů,
- metodika umožňuje komplexní zhodnocení a nalezení současných nedostatků, dále upozorňuje na pravděpodobné budoucí nedostatky, navrhuje konkrétní opatření, napomáhá tak eliminaci rizik,
- metodika umožňuje získat srovnání s obvyklými standardy a praktikami identifikovanými odborníky z praxe, je rozšiřitelná a obecná,
- metodika umožňuje odhalit shodu nebo neshodu se stanovenými postupy a identifikovat významná rizika nepokrytá proaktivními či reaktivními opatřeními,
- metodika umožňuje snížit četnosti výpadků IS/ICT a tím i ekonomických ztrát,
- pro malé firmy slouží jako ověření současného stavu v oblasti informačních systémů, pro středí a větší může také sloužit jako prověrka systémů před plánovaným auditem či jiným typem hodnocení (ISAE 3402 nebo SOX).

5.3 Přínosy pro pedagogickou praxi

Výsledky dizertační práce lze také využít pro pedagogickou praxi. Práce nabízí ucelený pohled na problematiku hodnocení informačních systémů od důkladné analýzy, přes stanovení kritérií až po ověření v praxi. Samotná metodika může být nejen předmětem výuky předmětů zaměřených na podnikovou informatiku, ale také využita v bakalářských či diplomových pracích vedených na Fakultě podnikatelské VUT v Brně. V tomto ohledu se rýsují dvě možnosti začlenění. První variantou je použití metodiky v práci zaměřené na posouzení informačního systému a návrhu změn do procesu analýzy informačního systému firmy. Druhou možností je návrh rozšíření metodiky o další oblasti nebo její zaměření na konkrétní obor podnikání či specifický informační systém. V tomto případě by pak bylo například možné metodiku přizpůsobit pro systém SAP a současně konkretizovat obecné požadavky pro tento rozšířený systém. Jelikož je metodika úzce spojena s řízením a auditem informačních systémů, může být nápomocna také ve vzdělávání budoucích manažerů informatiky, projektových IT manažerů či auditorů informačních systémů. Poptávka po těchto pozicích stále stoupá a sahá za hranice České republiky. Výuka tak může mít i mezinárodní rozměr a potenciál pro nadnárodní studentské aktivity. V oblasti pedagogiky přispívá práce především v:

- seznámení studentů s výsledky hloubkových rozhovorů a databází nedostatků a opatření,
- seznámení studentů s výsledky ověření metodiky v praxi a reálnými návrhy opatření v rámci případových studií,
- umožnění studentům oborů Řízení a ekonomika podniku a Informační management realizovaných při Fakultě podnikatelské VUT v Brně používat metodiku v praxi,
- využití výsledků dizertační práce jako zdroj pro výuku předmětů, které jsou spojeny s řízením informačních systémů a podnikovou informatikou, na Fakultě podnikatelské VUT v Brně to mohou být například Managment informačních systémů, Systémová integrace, Řízení životního cyklu IS, Podnikové informační systémy a Applied Informatics.

6 ZÁVĚR

Na řízení informací pomocí informačních systémů a informačních a komunikačních technologií je v současné době kladen velký důraz. Řada společností náležitě využila a stále využívá tento trend jako příležitost pro další rozvoj, získání nových trhů a jako prostředek pro zvyšování produktivity a kvality služeb. Spektrum služeb, které podnik dnes nabízí, se rozšiřuje právě díky IS/ICT, které otevírají nové trhy a prodejní kanály či tvoří novou přidanou hodnotu k současným službám a produktům. V posledních letech prochází výpočetní technologie prudkými změnami, na které musí organizace adekvátně reagovat. To v praxi znamená nejen obnovu technologií, ale často také změnu na všech úrovních řízení a v neposlední řadě také v odděleních podnikové informatiky. Pokrok v dané oblasti mění informační systémy a rozšiřuje možnosti jejich využívání. V důsledku rychlého technologického pokroku se stále více odhalují slabiny, mezi které patří neefektivní využívání informačních systémů, absence strategických plánů, chybějící podpora managementu nebo nezájem koncových uživatelů. **Roste proto i poptávka po nezávislé kontrole informačních systémů a souvisejících procesů s cílem využívat IS/ICT jako příležitosti a eliminovat související hrozby a slabé stránky.**

Svět podnikové informatiky je v současné době mimo jiné formován požadavky z mnoha oblastí zahrnující normy, zákony, standardy či statutární nebo jiné formy auditu. Rychlý růst investic do oblasti informačních systémů přináší tlak na řízení firmy, které musí brát v úvahu veškerá související rizika. V souladu se strategií a finančním plánováním rostou obavy manažerů také v oblasti bezpečnosti. Jakýkoli nedostatek totiž může mít velmi negativní dopad na chod celé organizace. Výběr správného řešení a snížení rizik může být klíčovým faktorem pro udržení životaschopnosti a prosperity firmy. **Na zmíněné trendy navazuje tato dizertační práce, která představuje komplexně zpracované téma v oblasti hodnocení informačních systémů.**

Dizertační práce je orientovaná na oblast hodnocení informačních systémů a vymezuje hlavní nedostatky v provozu a řízení informačních systémů v návaznosti na procesy v oddělení informatiky, s částečným přesahem do ostatních částí podniku. Výzkum prezentovaný v této dizertační práci se sestává ze tří po sobě jdoucích kroků: určení oblasti výzkumu a výzkumné otázky, návrh plánu výzkumu, provedení sběru dat a jejich analýza a sestavení

zprávy o výzkumu. Použité metody a současný stav vědeckého poznání prochází všemi výzkumnými kroky a slouží jako jeden ze základních kamenů práce. Výzkumný proces začíná definováním tématu práce a cíle práce. V souladu s výzkumnými otázkami byly následně uskutečněny a vyhodnoceny hloubkové rozhovory, jejichž provedení se sestává z několika kroků. Nejdříve byla sestavena a na malém vzorku otestována témata, následně byly provedeny rozhovory s odborníky z praxe a pomocí kódování vyhodnoceny. Výsledkem byl vznik databáze nedostatků obsahující detailní popis rizik a opatření. Na tomto základě byla sestavena metodika hodnocení informačních systémů skládající se ze šesti následujících fází: rozsah hodnocení, dotazníkové šetření, studium dokumentů, interview, vyhodnocení nedostatků a závěrečná zpráva. Metodika byla nejdříve otestována na malém vzorku a poté byla v souladu s druhou výzkumnou otázkou ověřena kvalitativním přístupem pomocí případových studií v malé, střední a velké společnosti. Obecným cílem metodiky je provést hodnocení ve velmi krátkém čase a odhalit podstatné nedostatky identifikované experty v této problematice. Očekávaným výsledkem je snížení nedostatků v oblasti informačních systémů a z toho pramenící důvěra a spoleh na informační systémy. V další fázi byly na základě dílčích zjištění sestaveny výsledky celého výzkumu.

Díky získaným výsledkům byl splněn cíl práce, zodpovězeny výzkumné otázky a formulovány přínosy práce. Byly zmapovány aktuální poznatky a identifikovány možnosti pro další výzkum a využití metodiky ve firemním prostředí. Dále byly stanoveny závěry vedoucí k eliminaci nedostatků v oblasti informačních systémů a v neposlední řadě k využití výsledků dizertační práce také v pedagogické praxi.

SEZNAM POUŽITÝCH ZDROJŮ

BOHUSLAV, Radim a Josef BASL, 2003. Inovace podnikových informačních systémů. *Systémová integrace.* 03, 321-327.

BODDY, David, Albert BOONSTRA a Graham KENNEDY, 2008. *Managing information systems: strategy and organisation*. 3rd ed. New York: Prentice Hall/Financial Times. ISBN 978-0273716815.

BOTCHKAREV, Alexei, Peter ANDRU a Raymond CHIONG, 2011. A Return on Investment as a Metric for Evaluating Information Systems: Taxonomy and Application. *Interdisciplinary Journal of Information, Knowledge*. 6, 245-269. ISSN 1555-1229.

BUCKSTEEG, Martin, 2012. *ITIL 2011*. Brno: Computer Press. 216 s. ISBN 978-80-251-3732-1.

BUDÍKOVÁ, Marie, Maria KRÁLOVÁ a Bohumil MAROŠ, 2010. *Průvodce základními statistickými metodami*. Praha: Grada. 272 s. ISBN 978-80-247-3243-5.

Bureau van Dijk, 2017a. *A database of comparable financial information for public and private companies across Europe*, [online]. [cit. 2017-03-01]. Dostupné z: http://amadeus.bvdinfo.com

Bureau van Dijk, 2017b. *Company size categories*, [online]. [cit. 2017-06-01]. Dostupné z: https://help.bvdinfo.com/mergedProjects/64_EN/Data/Coverage/CompSizeCat1.htm

COBIT introductory workshop, 2009. *Introduction to COBIT, its Role in IT Governance and How to Apply it In UCIT*, [online]. University of Calgary. [cit. 2017-02-01]. Dostupné z: https://www.vpit.ualberta.ca/.../ppt/cobit_ucalgary_workshop.ppt

COTS, Santi, Martí CASADESÚS a Frederic MARIMON, 2016. Benefits of ISO 20000 IT service management certification. *Information Systems and e-Business Management*. 14(1), 1-18. DOI: 10.1007/s10257-014-0271-2. ISSN 1617-9846.

CRISÓSTOMO, Javier, Luis FLORES, Karin MELENDEZ a Abraham DÁVILA, 2016. Convergence analysis of ISO/IEC 12207 and CMMI-DEV: A systematic literature review. *Computing Conference (CLEI)*, 2016 XLII Latin American. IEEE.

ČERVENÝ, Radim, Jiří FICBAUER, Alena HANZELKOVÁ a Miloslav KEŘKOVSKÝ, 2014. *Business plán: krok za krokem*. Praha: C.H. Beck. 240 s. ISBN 978-80-7400-511-4.

Český statistický úřad, 2017. *Klasifikace ekonomických činností dle NACE*, [online]. [cit. 2016-06-01]. Dostupné z: https://www.czso.cz/csu/czso/klasifikace_ekonomickych_cinnosti_cz_nace

CMMI Institute, 2017. *What Is Capability Maturity Model Integration (CMMI)*, [online]. [cit. 2017-03-15]. Dostupné z: http://cmmiinstitute.com/capability-maturity-model-integration

ČSN ISO 31000, 2010. *Management rizik – Principy a směrnice*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

DELONE William a Ephraim McLEAN, 1992. Information systems success: The quest for the dependent variable. *Information Systems Research*, 3(1), 60–95.

DELONE William a Ephraim McLEAN, 2003. The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *J. Manage. Inf. Syst.* 19, 4 (April 2003), 9-30.

DISMAN, Miroslav, 2011. *Jak se vyrábí sociologická znalost: příručka pro uživatele.* 4. vyd. Praha: Karolinum. 374 s. ISBN 80-246-0139-7.

DOHNAL, Jan a Oldřich PŘÍKLENK, 2011. *CIO a podpora byznysu: s případovými studiemi CIO v ČR a SR*. Praha: Grada. 176 s. ISBN 978-80-247-4050-8.

DOLEŽAL, Jan, Pavel MÁCHAL, Bronislav LACKO a kol., 2012. *Projektový management podle IPMA*. Praha: Grada Publishing, 526 s. ISBN 978-80-247-4275-5

DOSTÁL, Petr, Karel RAIS a Zdeněk SOJKA, 2005. *Pokročilé metody manažerského rozhodování: pro manažery, specialisty, podnikatele studenty, konkrétní příklady využití metod v praxi*. Praha: Grada Publishing, 168 s. ISBN 80-247-1338-1.

DOSTÁL, Petr, 2008. *Pokročilé metody analýz a modelování v podnikatelství a veřejné správě*. Brno: Akademické nakladatelství CERM, 430 s. ISBN 978-80-7204-605-8

DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ, 2008. *Řízení bezpečnosti informací*. Praha: Professional Publishing, 240 s. ISBN 978-80-86946-88-7.

DOVRTĚL, Jan, 2004. *Vybrané aspekty efektivnosti informačních systémů*. Dizertační práce. Brno. Vysoké učení technické v Brně, Fakulta podnikatelská.

DUNCAN, Bob a Mark WHITTINGTON, 2014. Compliance with standards, assurance and audit. *Proceedings of the 7th International Conference on Security of Information and Networks*. DOI: 10.1145/2659651.2659711.

DVOŘÁČEK, Jiří, 2005. *Audit podniku a jeho operací*. Praha: C. H. Beck, 168 s. ISBN 80-7179-809-6.

DRUCKER, Peter Ferdinand, 1993. *Postkapitalistická společnost*. Praha: Management Press. 197 s. ISBN 80-856-0331-4.

FOTR, Jiří a Ivan SOUČEK. 2005. *Podnikatelský záměr a investiční rozhodování*. Praha: Grada. 356 s. ISBN 80-247-0939-2.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ, 2015. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi.* 3., aktualiz. vyd. Praha: Grada Publishing, 240 s. ISBN 978-80-247-5457-4.

Gartner, 2014. *Total cost of ownership*, [online]. [cit. 2017-07-17]. Dostupné z: http://www.gartner.com/it-glossary/total-cost-of-ownership-tco

GEHRMANN, Maico, 2012. Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *Navus-Revista de Gestão e Tecnologia*. 2(2), 66-77. ISSN 2237-4558.

GROVER, Varun, Seung Ryul JEONG a Albert SEGARS, 1996. Information systems effectiveness: The construct space and patterns of application. *Journal of Management Information Systems*. 31(4), 177-191.

HAUFE, Kunt, Ricardo COLOMO-PALACIOS, Srdan DZOMBETA, Knud BRANDIS a Vladimir STANTCHEV, 2016. Security Management Standards: A Mapping. *Procedia Computer Science*, 100, 755-761. DOI 10.1016/j.procs.2016.09.221

HAYAT, Munawar a Rizwan Jameel QURESHI, 2016. Measuring the Effect of CMMI Quality Standard on Agile Scrum Model. *International Journal of Information Engineering and Electronic Business* 7(6), 46-52. DOI 10.5815/ijieeb

HENDL, Jan, 2015. *Přehled statistických metod: Analýza a metaanalýza dat*. 5. vyd. Praha: Portál, 736 s. ISBN 978-80-262-0981-2.

HENDL, Jan, 2016. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 4., aktualiz. vyd. Praha: Portál, 440 s. ISBN 978-80-262-0982-9.

HOSNAVI, Reza a Majid RAMEZAN, 2010. *Measuring the effectiveness of a human resource information system in National Iranian Oil Company: An empirical assessment*. Education, Business and Society: Contemporary Middle Eastern Issues, 3(1), pp.28-39. DOI 10.1108/17537981011022797

CHA-JAN CHANG, Jerry a William R. KING, 2005. Measuring the Performance of Information Systems: A Functional Scorecard. *J. Manage. Inf. Syst.* 22(1), 85-115. DOI: 10.1080/07421222.2003.11045833.

Information Security Forum, 2010. *Information Risk Assessment Methodology*, [online]. [cit. 2014-10-01]. Dostupné z: www.securityforum.org/page=DocuemntView&itemid=4414

IRANI, Zahir a Peter LOVE, 2008. *Evaluating Information Systems: Public and private sector*, Oxford: Elsevier. DOI: 10.1016/B978-0-7506-8587-0.50004-4

ISACA, 2007. *IT Governance Using COBIT® and Val ITTM: Student Book*. IT Governance Institute [online], 94 s. [cit. 2017-04-15]. ISBN 978-1-60420-024-9 Dostupné z: https://www.isaca.org/Membership/Academic-Membership/Documents/IT_Gov_Using_COBIT_and_ValIT_Student_Book_SAMPLE_Research.pdf

ISACA, 2008. *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 Extract*. IT Governance Institute [online], 43 s. [cit. 2017-04-15]. Dostupné z: https://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Val-IT-Framework-2.0-Extract-Jul-2008.pdf

ISACA, 2009. *The Risk IT Framework Excerpt*. IT Governance Institute, 106 s. [cit. 2017-04-15]. Dostupné z: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

ISACA, 2011. *Global Status Report on the Governance of Enterprise It (Geit)*. IT Governance Institute, 69 s. [cit. 2017-04-15]. Dostupné z: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/itgi-global-survey-results.aspx

ISACA, 2012. COBIT 5. *A Business Framework for the Governance and Management of Enterprise IT*. IT Governance Institute, 89 s. [cit. 2017-03-01]. ISBN 978-1-60420-237-3. Dostupné z: http://www.isaca.org/cobit/pages/default.aspx

ISACA, 2017. *ISACA Certification: IT Audit, Security, Governance and Risk*. [cit. 2017-07-17]. Dostupné z: http://www.isaca.org/certification/pages/default.aspx

JANÍČEK, Přemysl, 2007. *Systémové pojetí vybraných oborů pro techniky: hledání souvislostí*. Brno: Akademické nakladatelství CERM. 1380 s. ISBN 978-80-7204-554-9.

JANÍČEK, Přemysl a Jiří MAREK, 2013. *Expertní inženýrství v systémovém pojetí*. Praha: Grada. ISBN 978-802-4741-277.

JECH, Vladimír, 2010. *Dříve než se rozhodnete pro ten správný standard*, [online]. Středoevropské centrum pro finance a management. [cit. 2017-08-19]. Dostupné z: http://www.finance-management.cz/065textyVypis.php?IdTxtPass=16

KAFKA, Tomáš, 2009. *Průvodce pro interní audit a risk management*. Praha: C.H. Beck. ISBN 978-80-7400-121-5.

KAPLAN, Robert S. a David P. NORTON, 2010. *Efektivní systém řízení strategie: nový nástroj zvyšování výkonnosti a vytváření konkurenční výhody*. Praha: Management Press. ISBN 978-80-7261-203-1.

KEŘKOVSKÝ, Miloslav a Oldřich VYKYPĚL, 2006. *Strategické řízení: teorie pro praxi*. 2. vyd. Praha: C.H. Beck. 206 s. ISBN 80-717-9453-8.

KEŘKOVSKÝ, Miloslav, 2015. *IS/IT strategie krok za krokem: teorie pro praxi*. Praha: C.H. Beck. 208 s. ISBN 978-80-7400-272-4.

KIM, Dan J., Kwok-Bun YUE, Hisham AL-MUBAID, Sharon P. HALL a Krishani ABEYSEKERA, 2012. Assessing Information Systems and Computer Information Systems Programs from a Balanced Scorecard Perspective. *Journal of Information Systems Education*. 23(2). ISSN 1055-3096.

KOCH, Miloš, 2005. Možnosti využití metody HOS8 k posouzení efektivnosti informačního systému firmy. Progressive Methods and Tools of Management and Economics. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2005. s. 1-6. ISBN: 80-214-3099-0.

KOCH, Miloš, Jan DOVRTĚL, Tomáš HRŮZA a Hana NENIČKOVÁ, 2010. *Management informačních systémů*. 3., přeprac. vyd. Brno: Akademické nakladatelství CERM. ISBN 978-80-214-4157-6.

KOCH, Miloš, 2014. *ZEFIS – posouzení efektivnosti informačních systémů* [online]. [cit. 2017-08-19]. Dostupné z: http://www.zefis.cz

Komora auditorů České republiky, 2011. *Mezinárodní standard pro ověření zakázky ISAE 3402*, [online]. [cit. 2017-08-19]. Dostupné z: https://www.kacr.cz/data/Metodika/Auditing/Handbook%202010/2.%20%C4%8D%C3%A1st/ISAE%203402.pdf

Komora auditorů České republiky, 2016. *Auditorské standardy 2016,* [online]. [cit. 2017-08-19]. Dostupné z: https://www.kacr.cz/auditorske-standardy-2016

KOUDELA, Radek, 2011. *Hodnocení přístupů k analýze bezpečnostních rizik*. Praha. Diplomová práce. Vysoká škola ekonomická v Praze.

KOVANICOVÁ, Dana, 2007. *Je Sarbanes-Oxley Act tou správnou léčbou? (Diskuse k článku: Coates IV, John C.: The Goals and Promise of the SarbanesOxley Act. Journal of Economic Perspectives*). Český finanční a účetní časopis, 2008, roč. 3, č. 2.

KOZEL, Roman, Lenka MYNÁŘOVÁ a Hana SVOBODOVÁ, 2011. *Moderní metody a techniky marketingového výzkumu*. Praha: Grada. ISBN 978-802-4735-276.

KŘÍŽ, Jiří, 2001. *Problematika typologie a vyváženosti informačních systémů*. Brno. Dizertační práce. Vysoké učení technické v Brně.

LAGSTEN, Jenny, 2011. Evaluating Information Systems according to Stakeholders: A Pragmatic Perspective and Method. *Electronic Journal of Information Systems Evaluation*. 14(1), 73-88. ISSN 15666379.

LIŠKA, Václav, 2004. *Doctorandus: průvodce budoucích Ph.D*. Praha: Professional Publishing. ISBN 80-864-1960-6.

LOW, Chinyao a Ya CHEN, 2012. Criteria for the Evaluation of a Cloud-Based Hospital Information System Outsourcing Provider. *Journal of Medical Systems*. 36(6), 3543-3553. DOI: 10.1007/s10916-012-9829-z. ISSN 01485598.

LUKÁČ, Ľubomír, 2011. *IT management: jak na úspěšnou kariéru*. Brno: Computer Press. ISBN 978-80-251-3378-1.

MARYŠKA, Miloš, 2007. Měření ekonomické efektivnosti informačního systému. *Systémová integrace.* 07*, 85-98.* Dostupné z: http://www.cssi.cz/cssi/system/files/all/maryska.pdf

Ministerstvo financí České republiky, 2004. Kodexu správy a řízení společností [online]. [cit. 2016-10-15]. Dostupné z: http://www.mfcr.cz/cs/archiv/transformacni-instituce/agenda-byvaleho-fnm/sprava-majetku/kodex-spravy-a-rizeni-spolecnosti-corpor

MLÁDKOVÁ, Ludmila, 2005. *Moderní přístupy k managementu: tacitní znalost a jak ji řídit*. Praha: C.H. 195 s. ISBN 80-717-9310-8.

MOLNÁR, Zdeněk, Dušan PAVLÍK a Jaroslav VLASÁK, 1999. Efektivnost IS IT v podnicích České republiky. *Systémová integrace.* 99, 301-308.

MOLNÁR, Zdeněk, 2000. *Efektivnost informačních systémů*. Praha: Grada. ISBN 80-716-9410-X.

MOLNÁR, Zdeněk, 2011. *Úvod do základů vědecké práce: Sylabus pro potřeby semináře doktorandů* [online]. [cit. 2015-05-15]. Dostupné z: http://web.fame.utb.cz/cs/docs/Z__klady_v__deck___pr__ce.doc

MOLNÁR, Zdeněk, 2012. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting. ISBN 978-80-7259-064-3.

MUSHTAQUE, Khuram, Kamran AHSAN a Ahmer UMER, 2014. IT Governance in Banking Sector: VAL IT and Risk Assessment Perspective. *Science International*. 26(3), 1259-1264. ISSN 10135316.

NEUBAUER, Jiří, Marek SEDLAČÍK a Oldřich KŘÍŽ, 2016. *Základy statistiky: aplikace v technických a ekonomických oborech*. 2., rozšířené vydání. Praha: Grada. 280 s. ISBN 978-80-247-5786-5.

NEUWIRTH, Bernard, 2009. *Problematika typologie a vyváženosti informačních systémů*. Dizertační práce. Brno. Vysoké učení technické v Brně, Fakulta podnikatelská.

NOVÁK, Lukáš, 2012. *Metody hodnocení efektivnosti informačních systémů: základní analýza a srovnání vytvořených metod*. *Mezinárodní workshop doktorandských prací*. Vysoké učení technické v Brně. Fakulta podnikatelská.

NOVÁK, Lukáš, 2013. The relationship of the GDP and ICT Spending and Investment: Analysis of data between 2006 and 2011 in the Czech Republic. *Vision 2020: Innovation, Development Sustainability, and Economic Growth Proceedings.* Vienna: IBIMA.

NOVÁK, Lukáš, 2014a. Analysis of the Effect of Economic Development on Expenditures and Investments into IT in the Czech Republic, Poland, Slovakia and Hungary. *Vision 2020: Sustainable Growth, Economic Development, and Global Competitiveness*. Valencia: IBIMA.

NOVÁK, Lukáš, 2014b. The Success Factors in an International Company: A Case Study. *Crafting Global Competitive Economies: 2020 Vision Strategic Planning & Smart Implementation*. Miláno: IBIMA.

NOVÁK, Lukáš, 2015a. Development of an Information Strategy and Proposed Changes in Corporate Informatics on the Basis of an Application of Methods of Scientific Analysis to the Information System Evaluation: Case Study. *Innovation Vision 2020: From Regional Development Sustainability to Global Economic Growth.* Amsterdam: IBIMA.

NOVÁK, Lukáš, 2015b. Analysis of Methods for the Evaluation of Information Systems: Critical Comparison by Selected Criteria. Madrid: IBIMA.

NOVÁK, Lukáš, 2016. Evaluation of Information Systems in Medium – sized and Large Businesses. *International Scientific Conference Economics and Management.* Brno: Brno University of Technology.

OCHRANA, František, 2013. *Metodologie sociálních věd*. Praha: Karolinum. ISBN 978-802-4623-801.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK, 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM. 377 s. ISBN 978-80-7204-872-4.

PANOPOULOS, John, 2012. Integrating COBIT 4.1 Into the Internal Audit Function. *COBIT Focus* [online]. [cit. 2017-08-19]. Dostupné z: http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Integrating-COBIT-4-1-Into-the-Internal-Audit-Function.aspx

PATHER, Shaun, Dan REMENYI a Geoff ERWIN, 2003. Measuring e-Commerce effectiveness: a conceptual model. *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology (SAICSIT '03)*. South African Institute for Computer Scientists and Information Technologists, Republic of South Africa, 143-152.

PAVELKOVÁ, Drahomíra a Adriana KNÁPKOVÁ, 2012. *Výkonnost podniku z pohledu finančního manažera*. 3. vyd. Praha: Linde. ISBN 978-80-7201-872-7.

PUNCH, Keith, 2008. *Základy kvantitativního šetření*. Praha: Portál. ISBN 978-80-7367-381-9.

RAIS, Karel a Radek DOSKOČIL, 2007. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM. ISBN 978-80-214-3510-0.

RAIS, Karel a Radek DOSKOČIL, 2011. *Operační a systémová analýza I: studijní text pro prezenční a kombinovanou formu studia*. Brno: Akademické nakladatelství CERM. ISBN 978-80-214-4364-8.

REICHEL, Jiří, 2009. *Kapitoly metodologie sociálních výzkumů*. Praha: Grada. ISBN 978-80-247-3006-6.

REŽŇÁKOVÁ, Mária, 2005. *Finanční management: studijní text pro kombinovanou formu studia, 2. díl*. Brno: Akademické nakladatelství CERM. ISBN 80-214-3035-4.

Risk Analysis Consultants, 2017. *RAMSES: Řízení bezpečnosti informací organizace* [online]. [cit. 2017-02-15]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/Ramses

RYOO, Jungwoo, Syed RIZVI, William AIKEN a John KISSELL, 2014. Cloud Security Auditing: Challenges and Emerging Approaches. *IEEE Security*. 12(6), 68-74. DOI: 10.1109/MSP.2013.132. ISSN 1540-7993.

SAHIBUDIN Shamsul, Mohammad SHARIFI a Masarat AYAT, 2008. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. In *Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)* (AMS '08). IEEE Computer Society, 749-753. DOI 10.1109/AMS.2008.145

SÁNCHEZ PEÑA, Juan José, Eugenio FERNÁNDEZ VICENTE a Antonio Moratilla OCAÑA, 2013. ITIL, COBIT and EFQM: Can They Work Together? *International Journal of Combinatorial Optimization Problems*. 4(1), 54-64. ISSN 20071558.

SCOTT, Judy E., 1995. The measurement of information systems effectiveness. *ACM SIGMIS Database*. 26(1), 43-61. DOI: 10.1145/206476.206484. ISSN 00950033.

SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. ISBN 978-80-247-4644-9.

SODOMKA, Petr, 2002. Hodnocení efektivnosti ERP systémů. *Systémová integrace.* 02, 75-85.

SODOMKA, Petr a Hana KLČOVÁ, 2010. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press. ISBN 978-80-251-2878-7.

SOLIC, Kresimir, Hrvoje OCEVCIC a Marin GOLUB, 2015. The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers*. 55, 100-112. DOI: 10.1016/j.cose.2015.08.004. ISSN 01674048.

SOUČEK, Eduard, 2006. *Statistika pro ekonomy*. Praha: Vysoká škola ekonomie a managementu. ISBN 978-808-6730-066.

STAKE, Robert, 1995. *The art of case study research*. Thousand Oaks: Sage Publications. ISBN 978-0803957671.

STRAUSS, Anselm a Juliet CORBIN, 1999. *Základy kvalitativního výzkumu: postupy a techniky metody zakotvené teorie*. Brno: Sdružení Podané ruce. ISBN 80-858-3460-X.

SURYANI, Ni Putu Sri Merta, Gusti Made Arya SASMITA a I. Ketut Adi PURNAWAN, 2015. Audit of Accounting Information System using COBIT 4.1 Focus on Deliver and Support Domain. *Journal of Theoretical and Applied Information Technology*. 78.3: 456.

SVATÁ, Vlasta, 2011. *Audit informačního systému*. Praha: Professional Publishing. ISBN 978-80-7431-034-8.

SVOZILOVÁ, Alena, 2016. *Projektový management: systémový přístup k řízení projektů*. 3. aktualiz. a rozš. vyd. Praha: Grada Publishing. 424 s. ISBN 978-80-271-0075-0.

ŠIROKÝ, Jan, 2010. *Publikování a presentace výsledků vědy a výzkumu*. Olomouc: Moravská vysoká škola Olomouc. ISBN 978-80-87240-41-0.

ŠIROKÝ, Jan, 2011. *Tvoříme a publikujeme odborné texty*. Brno: Computer Press. ISBN 978-80-251-3510-5.

ŠVARCOVÁ, Ivana a Tomáš RAIN, 2011. *Informační management*. Praha: Alfa Nakladatelství. 183 s. ISBN 978-80-8719-740-0.

TAVAKOLI, Sanambar, Noraini Binti Abu TALIB a Ehsan Kish Hazrat SOLTAN, 2016. Enterprise Risk Management Adoption and Financial Benefits Creation: Examining the Contributions of COSO ERM Maturity and Board of Directors. *Journal of Soft Computing and Decision Support Systems*. 3(3), 13-19.

The Sarbanes–Oxley Act, 2002. An Act To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.107–204, 116 Stat. 745, enacted July 30, 2002 H.R. 3763 (107th).

THORP, John, 2008. Val IT Framework 2.0: Relationship Between COBIT and Val IT. *COBIT Focus*. 3, 3-6.

TÖPFER, Armin, 2008. *Six Sigma: koncepce a příklady pro řízení bez chyb*. Brno: Computer Press. ISBN 80-251-1766-9.

TRUNEČEK, Jan, 2004. *Management znalostí*. Praha: C.H. Beck. 131 s. ISBN 80-717-9884-3.

TVRDÍKOVÁ, Milena, 2008. Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů. Praha: Grada. 176 s. ISBN 978-80-247-2728-8.

UČEŇ, Pavel, 2001. *Metriky v informatice: jak objektivně zjistit přínosy informačního systému*. Praha: Grada. Management v informační společnosti. ISBN 80-247-0080-8.

VEBER, Jaromír, Marie HŮLOVÁ a Alena PLÁŠKOVÁ, 2010. *Management kvality, environmentu a bezpečnosti práce: legislativa, systémy, metody, praxe*. 2., aktualiz. vyd. Praha: Management Press. ISBN 978-807-2612-109.

VOCHOZKA, Marek a Petr MULAČ, 2012. *Podniková ekonomika*. Praha: Grada. ISBN 978-80-247-4372-1.

VYMĚTAL, Dominik, 2009. *Informační systémy v podnicích: teorie a praxe projektování*. Praha: Grada. ISBN 80-247-3046-4.

WAGNER, Jaroslav, 2009. *Měření výkonnosti: jak měřit, vyhodnocovat a využívat informace o podnikové výkonnosti*. Praha: Grada. ISBN 978-80-247-2924-4.

WAHYUDI, Mochamad a Arief DESWANDI, 2016. Audit Information systems Core Banking System Using ITIL v3 Case Study on BTPN Sharia Bank. *Journal of Theoretical and Applied Information Technology*. 87(1).

WACHNIK, Bartosz, 2012. An Analysis of the Problems Linked to Economic Evaluation of Management Support Information Systems in Poland on the Example of ERP/CRM Class Applications – Problem Analysis. *Proceedings of the European Conference on Information Management*. 325-333.

WILKIN, Carla, John CAMPBELL, Stephen MOORE a Wim VAN GREMBERGEN, 2013. Co-Creating Value from IT in a Contracted Public Sector Service Environment: Perspectives on COBIT and Val IT. *Journal of Information Systems*. 27(1), 283-306. DOI: 10.2308/isys-50355. ISSN 08887985.

YIN, Robert K., 2012. *Applications of case study research*. 3rd ed. Calif.: Sage. ISBN 978-1412989169.

SEZNAM POUŽITÝCH ZKRATEK

ACCA	Association of Chartered Certified Accountants
AITP	Association for Information Technology Professionals
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BS	British Standard
BSC	Balanced Scorecard
CAAT	Computer Assisted Audit Techniques
CERT	Computer Emergency Response Team
CGEIT	Certified in the Governance of Enterprise IT
CHIS	Cloud-based Hospital Information Systems
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee Sponsoring Organizations of the Treadway Commission
CPM	Corporate Performance Management
CRAMM	CCTA Risk Analysis and Management Methodology
CRISC	Certified in Risk and Information Systems Control
DRP	Disaster Recovery Plan
EMS	Environmental Management System
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
HIPAA	Health Insurance Portability and Accountability Act
IIA	Institute of Internal Auditors
IMS	Integrated Management System
INTOSAI	International Organization of Supreme Audit Institutions
IPTV	Internet Protocol Television
IS/ICT	Information System and Information and Communications Technology

ISA	International Standards for Auditing
ISACA	Information System Audit and Control Association
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
KAČR	Komora Auditorů České Republiky
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
PCAOB	Public Company Accounting Oversight Board
PDCA	Plan, Do, Check, Act
PMBOK	Project Management Body of Knowledge
PRINCE2	Projects in Controlled Environment
QMS	Quality Management System
RAMSES	Risk Analysis and Management System for Enhanced Security
ROA	Return on Assets
ROE	Return on Equity
ROI	Return on Investments
SIM	Society of Information Management
SLA	Service Level Agreement
SLM	Service Level Management
SLR	Service Level Requirement
SOC	System and Organization Controls
SOX	Sarbanes-Oxley Act
TCO	Total Cost of Ownership
TVO	Total Value of Ownership
UAT	User Acceptance Testing

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha 1 – Výsledky dotazníkového šetření v rámci pilotní studie

Dotazníkové šetření v pilotní studii – Podniková dimenze (otázky A1 – A4)

Otázka	Odpověď	Výsledek
A1. Kolik lidí zaměstnává vaše firma?	1–15 zaměstnanců	17 (26 %)
	16–50 zaměstnanců	10 (15 %)
	51–150 zaměstnanců	14 (22 %)
	151 a více zaměstnanců	24 (37 %)
	-	0 (0 %)
A2. Jakým způsobem je ve společnosti provozována IT podpora?	Interní IT oddělení	38 (58 %)
	Outsourcing – externí IT oddělení, obvykle měsíční platba	3 (5 %)
	Externisté, obvykle platba od výkonu	14 (22 %)
	Mix interního oddělení a outsourcingu	10 (15 %)
	-	0 (0 %)
A3. Kolik zaměstnanců má IT oddělení?	0 (Využíváme outsourcing)	13 (20 %)
	1–2 lidé	23 (35 %)
	3–4 lidé	6 (10 %)
	Více jak 5	23 (35 %)
	-	0 (0 %)
A4. Jaké jsou roční výdaje Vaší firmy na hardware (vyjádřené v % z ročního obratu firmy)?	0 % – 1 %	14 (22 %)
	1 % – 2 %	12 (18 %)
	2 % – 4 %	4 (6 %)
	více než 5 %	6 (9 %)
	Naše firma tento údaj nesleduje	29 (45 %)

Dotazníkové šetření v pilotní studii – Podniková dimenze (otázky A5 – A8)

Otázka	Odpověď	Výsledek
A5. Jaké jsou roční výdaje Vaší firmy na software (vyjádřené v % z ročního obratu firmy)?	0 % – 1 %	15 (23 %)
	1 % – 2 %	11 (17 %)
	2 % – 4 %	5 (8 %)
	Více než 5 %	8 (12 %)
	Naše firma tento údaj nesleduje	26 (40 %)
A6. Jaké jsou výdaje za implementaci a změny informačních systémů (vyjádřená v % z ročního obratu firmy)?	0 % – 1 %	15 (24 %)
	1 % – 2 %	10 (16 %)
	2 % – 4 %	4 (6 %)
	Více než 5 %	6 (9 %)
	Naše firma tento údaj nesleduje	29 (45 %)
A7. Jaká je roční cena údržby podnikové informatiky vyjádřené v % z ročního obratu firmy?	0 % – 1 %	22 (35 %)
	1 % – 2 %	9 (14 %)
	2 % – 4 %	5 (8 %)
	Více než 5 %	3 (5 %)
	Naše firma tento údaj nesleduje	24 (38 %)
A8. Jaké je průměrné stáří hardwarového vybavení společnosti?	Méně než jeden rok	0 (0 %)
	1–3 roky	34 (53 %)
	3–6 let	26 (41 %)
	Více než 6 let	4 (6 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Podniková dimenze (otázky A9 – A10)

Otázka	Odpověď	Výsledek
A9. Jaké je průměrné stáří softwarového vybavení společnosti?	Méně než jeden rok	3 (5 %)
	1–3 roky	36 (56 %)
	3–6 let	15 (23 %)
	Více než 6 let	10 (16 %)
	-	0 (0 %)
A10. Jsou outsourcingované služby kryty pomocí smluv SLA?	Ano, všechny	11 (17 %)
	Ano, většina	16 (25 %)
	Ne, žádná	7 (11 %)
	Ne, nepoužíváme outsourcing	30 (47 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Uživatelská dimenze (otázky B1 – B2)

Otázka	Odpověď	Výsledek
B1. Jsou brány v úvahu změny dle požadavků zaměstnanců?	Ano, požadavky zaměstnanců jsou brány v úvahu, po pečlivém zvážení se rozhodneme, zda je implementujeme	42 (68 %)
	Ano, požadavky jsou brány v úvahu, některé požadavky jsou implementovány bez schvalovacího řízení	10 (16 %)
	Ne, požadavky uživatelů nejsou brány v úvahu	10 (16 %)
	-	0 (0 %)
	-	0 (0 %)
B2. Jsou poskytována školení a návody k informačnímu systému?	Ano, dodavatel poskytuje školení i návody k informačnímu systému a firma je využívá	37 (59 %)
	Ano, firma pro školení využívá místo služeb dodavatele informačního systému služeb jiné společnosti	5 (8 %)
	Ne, dodavatel poskytuje školení i návody k informačnímu školení, firma je ale nevyužívá	14 (22 %)
	Ne, dodavatel neposkytuje školení ani návody k informačnímu školení	7 (11 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Uživatelská dimenze (otázky B3 – B6)

Otázka	Odpověď	Výsledek
B3. Jak snadné je používat informační systém bez pomoci kolegů, IT specialisty nebo help linky dodavatele informačního systému?	Velmi snadné, informační systém je velmi intuitivní	11 (17 %)
	Snadné s občasnými problémy	41 (65 %)
	Obtížné	10 (16 %)
	Velmi obtížné, pomoc je nutné volat velmi často	1 (2 %)
	-	0 (0 %)
B4. Neposkytuje systém příliš mnoho nepotřebných informací pro konkrétní pracovní pozici?	Ne, všechny informace jsou pro každou pracovní pozici důležité	11 (17 %)
	Některé informace jsou nadbytečné, práci to ale nevadí	35 (56 %)
	Ano, systém poskytuje i ty informace, jež některé pracovní pozice nevyužijí	10 (16 %)
	Systém není přizpůsobený pracovní pozici zaměstnance, poskytuje stejné prostředí a informace pro každého uživatele	7 (11 %)
	-	0 (0 %)
B5. Jsou všechny informace poskytované informačním systémem důležité pro konkrétní pracovní pozici?	Ano	14 (22 %)
	Spíše ano	24 (38 %)
	Některé informace důležité nejsou	23 (37 %)
	Ne	2 (3 %)
	-	0 (0 %)
B6. Mají uživatelé dostatečná oprávnění k provádění změn v informačním systému vzhledem k pracovní pozici ve firmě?	Uživatelé mají přesně stanovená oprávnění daná jejich pracovní pozicí, dle nastavení procesů	40 (63 %)
	Každý uživatel má nastavena oprávnění daná pracovní pozicí, v případě nouze je možné se přihlásit pod cizím účtem	8 (13 %)
	Všichni uživatelé mají v systému stejná oprávnění, ale svůj účet	10 (16 %)
	Existují pracovní pozice, které svůj účet sdílejí	5 (8 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Uživatelská dimenze (otázky B7 – B10)

Otázka	Odpověď	Výsledek
B7. Jak snadné a rychlé je najít konkrétní informaci v informačním systému?	Hledání jakékoli informace je velmi snadné	12 (20 %)
	Většina informací je snadno dostupných, některé méně potřebné je třeba hledat déle	46 (74 %)
	Jen málo informací je dostupných rychle a snadno	2 (3 %)
	Pro hledání jakékoli informace je rychlejší zeptat se kolegů nebo zavolat pomoc odborníka	2 (3 %)
	-	0 (0 %)
B8. Poskytuje informační systém nějakou možnost komunikace či spolupráce mezi zaměstnanci?	Ano	23 (37 %)
	Spíše ano	23 (37 %)
	Spíše ne	9 (14 %)
	Ne	8 (12 %)
	-	0 (0 %)
B9. Vede používání informačního systému k stresovým situacím?	Ne	14 (22 %)
	Spíše ne	40 (63 %)
	Spíše ano	8 (13 %)
	Ano	1 (2 %)
	-	0 (0 %)
B10. Jak snadné je opravit omyl zanesený do informačního systému?	Velmi snadné	29 (46 %)
	Opravit omyl lze, je to ale složitější	25 (40 %)
	Obtížné, omyl musí opravit nadřízený nebo zaměstnanec IT	8 (13 %)
	Obtížné, omyl musí opravit programátor systému	1 (1 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Provozní dimenze (otázky X1 – X4)

Otázka	Odpověď	Výsledek
X1. Jak často dochází k chybám při distribuci informací (např. ztráta záznamu)?	Vůbec, velmi neobvyklá situace	19 (30 %)
	Ojediněle, obvykle chyba uživatele či selhání hardwaru	41 (65 %)
	Často, informace je nutné zadávat vícekrát	3 (5 %)
	-	0 (0 %)
	-	0 (0 %)
X2. Jak často dochází ke zmatku či nečinnosti kvůli nedostatku informací z informačního systému?	Tato situace nenastává	22 (35 %)
	Častý případ	4 (6 %)
	Zřídka	37 (59 %)
	-	0 (0 %)
	-	0 (0 %)
X3. Jak často jsou data v informačním systému zálohována?	Je vytvořený plán zálohování, data se zálohují automaticky, frekvence zálohy odpovídá důležitosti dat	43 (68 %)
	Plán zálohování není vytvořený, data se zálohují automaticky, frekvence zálohy odpovídá důležitosti dat	10 (16 %)
	Plán zálohování není vytvořený, data se zálohují příležitostně	9 (14 %)
	Plán zálohování není vytvořený, data nezálohujeme	1 (2 %)
	-	0 (0 %)
X4. Jak snadné a rychlé je obnovit data ze zálohy?	Velmi snadné, všechna důležitá data pro chod firmy jsou zálohována	47 (75 %)
	Zálohována jsou jen některá data důležitá pro chod firmy – snadno obnovitelná, zbytek neobnovitelný	15 (24 %)
	Obtížné, data nejsou zálohována, hledá se poslední verze dokumentu na flash disku. Dokument se může i ztratit	1 (1 %)
	-	0 (0 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Provozní dimenze (otázky X5 – X8)

Otázka	Odpověď	Výsledek
X5. Jak rychle se informace šíří v rámci podniku?	Po zadání informace do IS je možné informaci ihned použít	61 (97 %)
	Rychlost šíření informace je velmi pomalá	2 (3 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)
X6. Jsou data a procedury uloženy spíše v informačním systému nebo je jejich znalost a zpracování závislé na konkrétním uživateli?	Data a procedury jsou jen málo závislé na uživatelích	44 (70 %)
	Firma je velmi závislá na uživatelích, všechny důležité informace i procedury umí uživatelé	19 (30 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)
X7. Jak rychle mohou být vydána rozhodnutí díky informačnímu systému?	Velmi rychle, IS poskytuje velmi přehledné a strukturované informace	44 (70 %)
	Rozhodnutí je časově náročnější. V některých situacích není zcela jednoduché se vyznat v informacích, které systém poskytuje	6 (10 %)
	Pro vydání rozhodnutí IS nepoužíváme	13 (20 %)
	-	0 (0 %)
	-	0 (0 %)
X8. Jak často jsou rozhodnutí vydaná na základě informací z informačního systému špatná nebo nepřesná?	Rozhodnutí jsou obvykle správná	47 (75 %)
	Máme problém při provedení rozhodnutí. Rozhodnutí jsou často nepřesná	2 (3 %)
	Pro vydání rozhodnutí informační systém nepoužíváme	14 (22 %)
	-	0 (0 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Provozní dimenze (otázky X9 – X10)

Otázka	Odpověď	Výsledek
X9. Jak často jsou data v sytému uložena duplicitně?	Data v systém nejsou duplicitně	52 (83 %)
	Stává se často, že v systému jsou stejná data několikrát	11 (17 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)
X10. Jak snadné je předávání informací mezi odděleními firmy?	Velmi snadné	37 (59 %)
	Snadné, systém poskytuje export dat	18 (29 %)
	Informace je snazší zavolat či sdělit ústně	8 (13 %)
	-	0 (0 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Strategická dimenze (otázky Y1 – Y2)

Otázka	Odpověď	Výsledek
Y1. Jak jednoduché je přizpůsobit systém novým potřebám firmy?	Velmi snadné	44 (70 %)
	Obtížné, firma disponuje systémem, jehož dodavatel nenabízí adekvátní podporu a rozšíření	19 (30 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)
Y2. Jsou implementované funkce adekvátní k účelu použití informačního systému?	Ano, všechny funkce podporují chod podniku	37 (59 %)
	Ne, některé funkce jsou nadbytečné	26 (41 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Strategická dimenze (otázky Y3 – Y6)

Otázka	Odpověď	Výsledek
Y3. Řeší informační systém problém, na který byl vybrán?	Ano	60 (95 %)
	Ne, část systému je natolik chybový, že je/bylo nutné přejít na alternativní řešení	2 (3 %)
	Ne, celý systém je natolik chybový, že je/bylo nutné přejít na alternativní řešení	1 (2 %)
	-	0 (0 %)
	-	0 (0 %)
Y4. Je definována a formalizována strategie podniku?	Ano, existuje dokument se strategií podniku	37 (60 %)
	Ano, není ale formalizována	22 (35 %)
	Ne	3 (5 %)
	-	0 (0 %)
	-	0 (0 %)
Y5. Je definována a formalizována IT strategie podniku?	Ano, IT strategie popisuje plán projektů a služeb	24 (38 %)
	Je definována strategie podniku, ale plán investic do IT chybí	10 (16 %)
	Strategie není formalizovaná, jen v hlavách manažerů	19 (31 %)
	Ne	9 (15 %)
	-	0 (0 %)
Y6. Jak snadné je současný IS rozšířit o další moduly nebo funkce?	Systém je velmi snadno rozšiřitelný	28 (45 %)
	Dodavatel poskytuje podporu, rozšíření přesto problematické	26 (42 %)
	Při integraci více systémů je rozšíření problematické	6 (10 %)
	Systém je zastaralý, dodavatel neposkytuje podporu, rozšíření je problematické	2 (3 %)
	-	0 (0 %)

Dotazníkové šetření v pilotní studii – Strategická dimenze (otázky Y7 – Y10)

Otázka	Odpověď	Výsledek
Y7. Je možné docílit přímý ekonomický zisk díky nasazení informačního systému (např. zvýšení zisku firmy)?	Ano	40 (63 %)
	Ne	23 (37 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)
Y8. Jsou při hodnocení investice do informačních systémů zvažovány nepřímé ekonomické přínosy (např. zrychlení komunikace ve společnosti)?	Ano, v naší firmě zvažujeme i nepřímé přínosy ze zavedení informačního systému	44 (70 %)
	Nepřímé přínosy nejsou do hodnocení investice do informačních systému zahrnuty	19 (30 %)
	-	0 (0 %)
	-	0 (0 %)
	-	0 (0 %)
Y9. Jakým způsobem jsou prováděny a zpracovávány kontroly a hodnocení podnikové informatiky?	Kontroly provádí pravidelně externí auditorská firma	5 (8 %)
	Kontrolu provádí IT oddělení firmy nebo externisté, kteří se o IT starají	28 (44 %)
	Kontroly se provádí až při výskytu problémů	18 (29 %)
	Kontroly se neprovádí	12 (19 %)
	-	0 (0 %)
Y10. Podporuje hardware budoucí potřeby společnosti?	Ano, díky strategii máme naplánované využití hardwaru tak, aby podporoval potřeby firmy	32 (52 %)
	Není jasné, jak se bude firma rozvíjet, nelze to určit	21 (35 %)
	Je naplánována strategie, současný hardware nevyhovuje, počítá se s investicemi	3 (5 %)
	Jsou naplánované změny ve firmě, podporou hardwaru se nikdo nezabývá	5 (8 %)
	-	0 (0 %)

Příloha 2 – Průvodní otázky použité při hloubkových rozhovorech

1. Jaká je Vaše role v hodnocení informačních systémů?
2. Jaké oblasti jsou dle Vašeho názoru důležité pro hodnocení informačních systémů? Jaké oblasti jsou nejvíce podceňovány, jaké přeceňovány?
3. Jakou posloupnost kroků považujete za nejvhodnější pro provedení hodnocení?
4. Jaké jsou největší nedostatky v oblasti hodnocení informačních systémů? S jakými nejčastějšími a nejméně častými nedostatky jste se doposud setkal/a?
5. Jaké jsou obvyklé příčiny nedostatků, se kterými jste se setkal/a?
6. Jak často se využívá nějaká forma hodnocení informačních systémů ve firmách/ projektech, kterých jste byl/a součástí?
7. Jakým způsobem a kým je hodnocení informačních systémů řízeno?
8. Jaký vidíte přínos v hodnocení informačních systémů? Jaká vidíte slabá místa v současném přístupu k hodnocení informačních systémů?
9. Jaké jsou kritické faktory úspěchu hodnocení informačních systémů? Jaká rizika mohou působit na úspěch hodnocení?
10. S jakým přístupem jste se setkal/a při vyhodnocování nedostatků v oblasti informačních systémů?
11. Jaké jsou odlišnosti v metodikách pro hodnocení informačních systémů v různých odvětvích podnikání?
12. Jaké dokumenty je potřeba analyzovat pro zdárné hodnocení informačních systémů?
13. Jak dlouho trvá provedení hodnocení informačních systémů? Jaké faktory ovlivňují dobu trvání?
14. Jaké nástroje využíváte pro hodnocení informačních systémů? Jak složité je hodnotit informační systém dle metodiky, kterou používáte? Jak rychle si ji lze osvojit?
15. Jaké vnitřní a vnější faktory ovlivňují hodnocení informačních systémů?

Příloha 3 – Databáze nedostatků a návrhů opatření

G1. IT politiky nejsou formálně dokumentovány, schváleny a publikovány

Doména Organizace IT oddělení / Politiky a směrnice v oblasti IS/ICT

Popis Oficiální politiky a postupy v oblasti IS/ICT nebyly zavedeny, aktualizovány a komunikovány uživatelům.

Riziko Bez řádně dokumentovaných politik nemůže vedení zajistit, že jsou operační postupy jasně definovány, pochopeny a implementovány. Pokud neexistuje žádný formálně definovaný a zdokumentovaný proces, mohou být některé důležité kroky úmyslně nebo neúmyslně vynechány nebo ignorovány. Politiky a postupy slouží navíc jako kritický nástroj pro předávání poznatků novým zaměstnancům.

Doporučení Obecné politiky v IT by měli být řádně udržovány, formalizovány a schváleny vedením pro všechny významné systémy a procesy.

G2. Podnik nemá ucelenou strategii vedení a správy společnosti

Doména Organizace IT oddělení / Řízení IT oddělení

Popis Podnik neměl ucelenou strategii vedení a správy společnosti, která by byla dostatečně a pravidelně komunikována zaměstnancům podniku.

Riziko Nedostatečná úroveň Corporate governance zvyšuje riziko porušení vnitřních kontrolních mechanismů a nekalého jednání.

Doporučení Zvýšit úroveň Corporate governance v podniku tak, aby odpovídal společnosti obdobné velikosti.

G3. Nedostatečné řízení rizik v oblasti IS/ICT

Doména Organizace IT oddělení / Řízení IT oddělení

Popis Společnost neměla zavedené formální hodnocení rizik v oblasti IS/ICT s jasně definovanou metodikou pro hodnocení rizik založenou na business kritériích.

Riziko Bez pravidelně zdokumentovaného a aktualizovaného posouzení rizik v oblasti IS/ICT společnost nemusí být schopna zajistit, aby byla zachycena a řízena všechna významná rizika spojená s IS/ICT.

Doporučení Provedení vyhodnocení rizik v oblasti IS/ICT s cílem včas identifikovat potenciální hrozby a rizika. Analýza rizik by se měla minimálně zaměřit na kritické systémy a aplikace a zálohování systémů. Posouzení rizik by mělo sloužit jako základ pro vypracování BCP a DRP plánů.

G4. IT oddělení není řízeno centrálně a nezodpovídá za některé IS/ICT oblasti

Doména Organizace IT oddělení / Řízení IT oddělení

Popis IT oddělení nebylo řízeno centrálně a nezodpovídalo za některé IT oblasti.

Riziko Zatížení zaměstnanců (nelze být expertem v několika oblastech), spoléhání se na klíčové zaměstnance (problémy při ztrátě zaměstnance s klíčovými funkcemi), neefektivní řízení IT, jehož funkce jsou distribuovány ve více odděleních, obtížné sledování IT a podnikové strategie.

Doporučení Sjednotit správu IT infrastruktury napříč firmou, stanovit IT manažera, který bude mít na starosti pouze IT oddělení a provést analýzu IT rizik.

A1. V produkčním systému je aktivní a užívaný účet, který není schválený

Doména Přístupová oprávnění / Přidělování a odebírání uživatelských oprávnění

Popis V produkčním systému se nacházel účet, který nebyl formálně schválený.

Riziko Těmito účty mohou být provedeny neoprávněné operace nebo změny finančních údajů.

Doporučení Formalizovat správu přístupových práv.

A2. Proces udělování a odebírání přístupových oprávnění není řádně nastaven

Doména Přístupová oprávnění / Přidělování a odebírání uživatelských oprávnění

Popis Ve firmě neexistovali žádné formální důkazy týkající se změny uživatelských práv. Žádost o změnu přístupových práv uživatele byla obvykle prováděna na základě neformální žádosti (e-mailu, telefonu).

Riziko Změna přístupových práv uživatelů nemusí být náležitě schválena odpovědnými pracovníky, protože neexistují žádné formální důkazy. Nedostatečná kontrola přístupu uživatelů k aplikacím a datům může vést k neoprávněné manipulaci nebo úpravě dat.

Doporučení Zavedení formálního postupu pro změnu uživatelských přístupových práv a jejich schválení podložené písemnou žádostí.

A3. Žádosti o přidělení přístupových oprávnění nejsou řádně zdokumentovány

Doména Přístupová oprávnění / Přidělování a odebírání uživatelských oprávnění

Popis Neexistoval formální proces udělování přístupových práv. Pokud zaměstnanec opustil společnost, účet obvykle nebyl blokován, ale používal ho nový pracovník.

Riziko Není možné zjistit identitu uživatele v systému.

Doporučení Formalizovat správu přístupových práv. Osvědčený postup v případě odchodu zaměstnance z firmy je blokovat stávající uživatelský účet a pro nového pracovníka vytvořit nový.

A4. V produkčním systému je aktivní a užívaný účet zaměstnance, který již ve společnosti nepracuje

Doména Přístupová oprávnění / Přidělování a odebírání uživatelských oprávnění

Popis V systému existoval aktivní účet, který patřil zaměstnanci, který již společnost opustil. Navíc byl tento účet po odchodu zaměstnance využit pro přihlášení do systému.

Riziko Aktivní účty odchozích zaměstnanců zvyšují riziko neautorizovaného zásahu do systému, který může vést k narušení integrity dat nebo porušení důvěrnosti dat.

Doporučení Po odchodu zaměstnance je nutné okamžitě odebrat nebo zablokovat přístupová oprávnění.

A5. Uživatelské účty nejsou odebrány včas

Doména Přístupová oprávnění / Přidělování a odebírání uživatelských oprávnění

Popis Ačkoli by měl být všem zaměstnancům po ukončení jejich pracovního poměru zamezen přístup do systému, v systému byly účty odchozích pracovníků stále aktivní.

Riziko Neblokováním či nesmazáním přístupových účtů bývalých zaměstnancům v nejkratší možné době se zvyšuje riziko nepovoleného přístupu k aplikaci a k citlivým datům, které může vést k úmyslné změně dat či jejich smazání. To může vést až k nedůvěryhodnosti finančních dat.

Doporučení K incidentu obvykle dochází zejména kvůli nedostatku komunikace vůči IT oddělení. Bylo by vhodné zvážit posílení mechanismů, které zajistí včasný přenos informací o potřebě zablokování nebo smazání účtů.

A6. Není prováděna periodická kontrola přístupových oprávnění

Doména Přístupová oprávnění / Pravidelná kontrola uživatelských oprávnění

Popis Ve společnosti nebyla prováděna žádná periodická revize uživatelských účtů a přístupových práv.

Riziko Neprováděním pravidelné kontroly přístupových práv uživatelů se zvyšuje riziko, že uživatelská práva nejsou odpovídajícím způsobem nastavena nebo jsou změněna oproti původnímu nastavení. To může vést k tomu, že uživatelé mají přístup k údajům, které neodpovídají jejich pozici a povinnostem, a posléze k neoprávněné úpravě dat.

Doporučení Provádět nejméně každoroční kontrolu přístupových práv uživatelů, aby bylo možné zjistit, že uživatelům budou přidělena správná práva.

A7. Periodická kontrola přístupových oprávnění není formalizovaná

Doména Přístupová oprávnění / Pravidelná kontrola uživatelských oprávnění

Popis Pravidelná kontrola přístupových oprávnění byla prováděna pouze neformálně.

Riziko Zvyšuje se riziko neautorizovaných změn v systému, které mohou vést k výpadkům systému, případně ke ztrátě dat.

Doporučení Formalizovat proces pravidelné kontroly přístupových oprávnění, ve které by byl dokumentován průběh kontroly.

A8. Periodická kontrola přístupových oprávnění není dostatečná

Doména Přístupová oprávnění / Pravidelná kontrola uživatelských oprávnění

Popis Společnost prováděla pouze periodickou kontrolu uživatelských účtů. Není prováděna kontrola uživatelských oprávnění.

Riziko Pravidelné kontroly přístupových práv jsou prováděny, aby uživatelé měli dostatečný přístup k výkonu svých pracovních povinností. Bez pravidelné kontroly přístupových práv mohou mít uživatelé přístup k více oprávněním, než je požadováno (např. situace, kdy byl zaměstnanec převedeny z jednoho oddělení do jiného), což vede k potenciálnímu riziku úmyslné a nezjistitelné manipulace s finančními údaji.

Doporučení Kontrolovat oprávnění v systému pro každého uživatele.

A9. Uživatelé mají přístup k citlivým transakcím

Doména Přístupová oprávnění / Rozdělení pravomocí

Popis Velký počet uživatelů měl přístup k omezeným bezpečnostním činnostem v systému s následujícími schopnostmi: vytvořit účet, přiřadit profily a role, obnovit heslo, obnovit výrobní nastavení, import změn do produkce nebo údržbu databáze.

Riziko Uživatelé s takovými oprávněními mohou obejít všechny autorizační objekty a v důsledku toho mají možnost provádět úpravy nastavení programů a dat. Taková oprávnění mohou vést k podvodnému chování, neočekávanému chování systému, a nakonec k nespolehlivosti dat. Navíc může dojít k selhání systému.

Doporučení Provést kontrolu uživatelských rolí a přístupů uživatelů v systému a uplatnění odpovídajících změn v koncepci přidělování oprávnění. Kritická práva přístupu by měla být přiřazena velmi restriktivně a počet uživatelů, kteří mají přístup k těmto transakcím, by měl být omezen a schválen.

A10. Není zpracována matice neslučitelných oprávnění

Doména Přístupová oprávnění / Rozdělení pravomocí

Popis V rámci informačního systému nebyla zpracována matice neslučitelných oprávnění.

Riziko Hrozí zde riziko neoprávněného přístupu, zneužití informací či zpronevěry.

Doporučení Zpracování matice neslučitelných oprávnění pro informační systém. Zavést automatickou kontrolu čtyř očí pro rizikové operace (např. změna čísla bankovního účtu dodavatele a odběratele).

A11. Nedostatečné nastavení heslové politiky

Doména Přístupová oprávnění / Heslová politika

Popis Heslová politika nebyla nastaveno dle doporučených postupů.

Riziko Nastavení hesel tvoří základ pro prostředí kontroly bezpečnosti informací a nastavuje standardy pro ochranu informačních prostředků společnosti. Bez formální bezpečnostní infrastruktury se zvyšuje riziko neoprávněného přístupu k systémům a datům společnosti. Použití běžných nebo snadno odhadovaných hesel představuje riziko neoprávněného přístupu do systému.

Doporučení Měly by být zavedeny zásady osvědčených postupů v oblasti hesel: délka hesla alespoň osm znaků, zablokování účtu po pěti neúspěšných pokusech o přihlášení, zakázat opakovaného použití hesla, změna hesla alespoň každých 90 dní (nebo využít dvoufaktorové zabezpečení).

A12. Sdílený administrátorský účet

Doména Přístupová oprávnění / Administrátorské účty

Popis Pro správu informačního systému / databáze byl používán sdílený účet. Při využívání sdílených administrátorských účtů není možné zpětně identifikovat osobu, která pod daným účtem vystupovala.

Riziko Zvyšuje se riziko neautorizovaných změn v systému, které mohou vést k výpadkům systému, případně ke ztrátě dat.

Doporučení Zavést personifikované účty pro každého administrátora systému. Sdílený účet zablokovat nebo omezit tak, že k němu bude mít přístup pouze jedna osoba.

A13. Uživatelé s neomezeným oprávněním

Doména Přístupová oprávnění / Administrátorské účty

Popis Informační systém nebyl optimálně nastaven. V systému se nachází více uživatelů s neomezeným profilem (v systému SAP jde o SAP_ALL a SAP_NEW). Tyto profily znamenají neomezený administrátorský přístup do všech modulů pro čtení i pro zápis, včetně účtování, vývoje změn přímo v systému, administrace nebo i smazání celého informačního systému.

Riziko Používání těchto neomezených oprávnění pravděpodobně vyplývá z neexistence nebo nefunkčnosti autorizačního konceptu a tato situace by měla být co nejdříve napravena, protože v souvislosti s vypnutým logováním a slabou heslovou politikou v informačním systému to velmi komplikuje dohledatelnost v případě zneužití a hrozí zde riziko neoprávněné nebo nechtěné manipulace s daty a riziko zpronevěry. Zároveň tyto profily vylučují rozdělení pravomocí, protože umožnují neomezený přístup do informačního systému.

Doporučení Profil s neomezeným přístupem by měl mít podle používané praxe pouze jeden uživatel, který je zablokovaný a heslo k němu je uložené v trezoru a měl by být využíván pouze v krizových situacích nebo upgradech. Ostatním uživatelům by měla být přidělena oprávnění podle jejich pracovní náplně.

A14. Nedostatečné monitorování aktivit privilegovaných účtů

Doména Přístupová oprávnění / Administrátorské účty

Popis Činnost administrátorských účtů nebyla řádně monitorována, případné změny nebylo možné dohledat.

Riziko Výše uvedené zjištění zvyšuje riziko vzniku nežádoucích změn v datech, což může mít v konečném důsledku za následek problémy s jejich případnou přesností, kompletností, integritou či dostupností.

Doporučení Zvážit kroky vedoucí k posílení v oblasti bezpečnosti např. logování změn provedených na úrovni databáze, zejména do citlivých údajů např. účetnictví nebo čísla bankovních účtů.

A15. Vzdálený přístup do produkčního systému není monitorován

Doména Přístupová oprávnění / Vzdálený přístup

Popis Někteří uživatelé měli vzdálený přístup k produkčnímu systému. Vzájemná komunikace mezi klientem a serverem nebyla šifrována.

Riziko Nešifrovaná komunikace klient-server je zranitelná hlavně útokem typu „*Man in the middle"*. Protože uživatelské ID a hesla jsou odesílány nezabezpečeným způsobem, útočník by mohl získat přihlašovací údaje. Existuje značné riziko neoprávněného přístupu do produkčního prostředí a změn finančních a nefinančních údajů.

Doporučení Implementovat software pro šifrování komunikace mezi vzdálenými pracovními stanicemi a serverem.

C1. Proces změnového řízení není řádně nastaven

Doména Změnové řízení / Proces změnového řízení

Popis Společnost neměla formalizovaný proces řízení změn.

Riziko Bez politiky týkající se změnového řízení nemůže vedení zajistit, aby byly postupy jasně definovány, pochopeny a implementovány. Pokud neexistuje žádný formálně definovaný a zdokumentovaný proces změnového řízení, některé důležité kroky (např. testování) mohou být úmyslně nebo neúmyslně vynechány z cyklu změny programu, což může nakonec vést k neočekávanému chování aplikace. Navíc aktualizované politiky a postupy slouží jako kritický nástroj pro předávání poznatků o procesu ostatním zaměstnancům.

Doporučení Vedení by mělo zvážit dokumentování formálních politik a postupů pro změnové řízení pro prostředí informačních technologií. Tato dokumentace by měla pokrývat následující oblasti: proces zadání změnových požadavků, prioritizaci a sledování změny, řízení verzí, unit testing, integrační testy a UAT *(User Acceptance Testing),* autorizaci pro migraci změny do produkce, uživatelskou a technickou dokumentace a školení.

C2. Změna není testovaná před implementací do produkčního prostředí

Doména Změnové řízení / Proces změnového řízení

Popis Některé změny nebyly před implementací testovány.

Riziko Bez správných testovacích postupů existuje riziko selhání systému, které může způsobit finanční ztráty, nepřístupnost nebo ztrátu finančních údajů. Nedostatky v zálohovacích postupech zvyšují toto riziko.

Doporučení Před implementací do produkčního prostředí testovat jakékoli změny.

C3. Nedostatečné rozdělení pravomocí v oblasti změnového řízení

Doména Změnové řízení / Proces změnového řízení

Popis Nedostatečné oddělení povinností v procesu vývoje a testování nových vylepšení. V jednom nebo více případech došlo k naprogramování, otestování a migraci změny do produkce jednou osobou.

Riziko Oddělení pravomocí v rámci procesu řízení změn snižuje riziko provedení změny, která nebyla řádně testována a autorizována, což může vést k poškození dat nebo k poškození funkčnosti programu.

Doporučení Změny by měl provést jiný zaměstnanec než vývojář. Mohl by to být správce systému, který nemůže změnit kód programu. Další možností může být provedení změn prostřednictvím instalačních balíčků, které by byly nainstalovány / implementovány do zkušebního prostředí a po provedení testů by se stejný balíček instaloval na produkčního prostředí. Řešením by mohlo být také zavedení kontroly, v níž by operace jako vložení nebo úprava dat v klíčových tabulkách byly prověřeny odpovědnými pracovníky.

C4. Změny jsou implementovány bez testování přímo do produkce

Doména Změnové řízení / Proces změnového řízení

Popis Pro informační systém není vytvořeno testovací prostředí a prováděné změny byly prováděny přímo v produkčním prostředí, tzn. bez otestování.

Riziko Vysoké riziko implementace neotestovaných nebo neoprávněných změn do produkčního prostředí, které mohou mít vliv na konzistenci dat a funkčnost celého systému.

Doporučení Zavést testovací prostředí pro všechny finančně významné aplikace. Alespoň částečně (určit pro jaké druhy změn) formalizovat změnové řízení a vyžadovat tzv. Business case (přínosy změny vs. náklady na vývoj). Zavést pravidelné setkání IT a business týmů pro prioritizaci požadavků.

C5. Neomezený přístup interních vývojářů do produkčního prostředí

Doména Změnové řízení / Přístup do produkčního prostředí

Popis Vývojáři měli neomezený přístup do produkčního prostředí.

Riziko Je zde vysoké riziko implementace neotestovaných nebo neoprávněných změn do produkčního prostředí, které mohou mít vliv na konzistenci dat a funkčnost systému.

Doporučení Je nezbytné vypnout nebo zablokovat účty vývojářů v produkčním prostředí. Pro nouzové případy by měl být použit havarijní účet, k němuž by měl být přístup omezen a udělen formálně, pouze v odůvodněných případech a po nezbytnou dobu.

C6. Neomezený přístup dodavatele do produkčního prostředí

Doména Změnové řízení / Přístup do produkčního prostředí

Popis Servisní organizace měla plný přístup do produkčního prostředí.

Riziko V případě nedostatku kontroly nad přístupem externích stran se zvyšuje riziko, že může dojít náhodně nebo úmyslně k neoprávněným změnám.

Doporučení Zavést postupy, které posílí kontrolu společnosti nad vzdáleným přístupem externí servisní společnosti k aplikacím. Například vyhodnocení protokolů zavedených změn provedených externími stranami. Přístup externí strany by měl být také specifikován ve smlouvě (SLA).

O1. Nedostatečné monitorování rozhraní mezi aplikacemi

Doména Provoz IT / Rozhraní mezi aplikacemi

Popis Přenos dat mezi systémy probíhal manuálně. Navíc důkazy o monitorování rozhraní nebyly k dispozici.

Riziko Existuje riziko, že data nebyla úplně a přesně předána.

Doporučení Provádět kontrolu přenosu dat a uchovávat formální dokumentaci.

O2. Proces zálohování dat je nedostatečný

Doména Provoz IT / Zálohování

Popis Bylo zjištěno, že všechny záložní pásky byly uloženy v rámci firmy.

Riziko V případě nouzového stavu (např. požár v serverovně) může společnost ztratit všechna produkční data.

Doporučení Záložní pásky by měly být uloženy mimo lokalitu firmy.

O3. Nedostatečné testování záloh

Doména Provoz IT / Zálohování

Popis Zálohy nejsou zpětně testovány.

Riziko V případě nouze může společnost ztratit všechna produkční data.

Doporučení Provádět testy záloh v rámci testování DRP plánu.

O4. Zastaralá infrastruktura

Doména Provoz IT / Plán obnovy v případě provozních problémů

Popis Stará hardwarová a softwarová infrastruktura.

Riziko Starý a neaktualizovaný software může být nebezpečný a náchylný ke kybernetickým útokům.

Doporučení Zvážit obnovení staré infrastruktury. Nový hardware může zvýšit produktivitu zaměstnanců.

O5. Není implementován havarijní plán a plán kontinuity obchodních činností

Doména Provoz IT / Plán obnovy v případě provozních problémů

Popis Ve společnosti byly zjištěny nedostatky v oblasti zabezpečení chodu některých systémů. Společnost nemá formalizovány Havarijní plán DRP *(Disaster Recovery Plan)* a Plán kontinuity obchodních činností BCP *(Business Continuity Plan)*, které by jí umožnili efektivně řídit kontinuitu činností v oblasti financí a dalších podpůrných procesů. Nebyla také provedena Analýza dopadu BIA *(Business Impact Analysis)*.

Riziko Absence zavedeného a řádně otestovaného DRP a BCP může vést ke zpoždění při obnově kritických obchodních procesů a systémů, a tím v konečném důsledku k možnosti narušení důvěrnosti dat, integrity dat a zpoždění v dostupnosti dat. Dále není známo, jakých procesů by se případné výpadky dotknuli a jak by výpadek ovlivnil chod firmy.

Doporučení Připravit plány DRP a BCP pro lokální servery a procesy, tak aby bylo v případě nenadálé události možná obnova bez průtahů, v souladu s požadavky společnosti a bez větších finančních ztrát. Analýza rizik by měla sloužit jako základ pro vývoj BCP a DRP. Další vstup pro vývoj BCP a DRP by měla být Analýza dopadu na podnik *(Business Impact Analysis)*, která by měla identifikovat všechny klíčové procesy společnosti a aplikace na lokálním serveru. DRP by měl alespoň popisovat opatření v případě havárie, například: záložní středisko a procedury, kontakty pro partnery a poskytovatele služeb, role a rozdělení odpovědností, definice kritické doby, po kterou mohou být systémy mimo provoz, definice nastavení a jednotlivých kroků při obnově systémů. Vedení by mělo také zvážit podporu přípravy odpovídajícího Plánu obnovy obchodních činností BCP. Typicky by měl plán obsahovat alespoň analýzu klíčových procesů, analýzu každého systému a času, po který je možné, aby byl systém vypnutý bez vážného dopadu, rizika, kterým jsou jednotlivé systémy vystaveny, detailně popsané procedury pro obnovu systému v případě jeho výpadku, odpovědnosti specifikované pro každého zaměstnance v rámci procedur a nezbytné bezpečnostní požadavky, které musí být dodrženy při procesu obnovy. Plány by měly být pravidelně aktualizované a testované.

O6. Havarijní plán a plán kontinuity nepokrývají všechna rizika

Doména Provoz IT / Plán obnovy v případě provozních problémů

Popis BPC a DRP plány nepokrývají rizika spojená s výpadkem systémů. Tyto plány byly navrženy pouze pro částečný výpadek.

Riziko Bez zavedených a řádně testovaných nástrojů DRP a BCP se při obnově klíčových obchodních procesů a systémů mohou objevit zbytečná zpoždění, což může vést k finanční ztrátě.

Doporučení Podrobněji rozvíjet DRP i BCP.

O7. Fyzická bezpečnost serverovny

Doména Provoz IT / Fyzická bezpečnost

Popis V místnosti se servery chybělo požární čidlo.

Riziko V případě požáru by nemuselo dojít ke včasné detekci a uhašení požáru, čímž by mohlo dojít k nenávratnému poškození serverů a dále také k poškození budovy, ve které se serverovna nachází.

Doporučení Je nezbytné do serverovny nainstalovat požární hlásič, který by upozornil na nebezpečí požáru.

O8. Vypnuté logování produkční databáze

Doména Provoz IT / Logování

Popis Auditní log produkční databáze pro aplikace není zapnutý. To znamená, že aktivity administrátorů databáze nebyly logovány a neexistuje auditní stopa.

Riziko Zvýšené riziko neoprávněných zásahů v produkčních databázích finančně významných systémů a neexistence auditní stopy.

Doporučení Zapnutí logování produkční databáze může zvýšit zátěž, obzvláště u obrovských databází, ale aktivity administrátorů by měly být logovány. Proto je doporučováno, po interním vyhodnocení dopadů, zapnout logování minimálně na produkční databázi a auditní logy by měly být ukládány na server, kam administrátoři nemají přístup.

Příloha 4 – Podklady pro metodiku hodnocení informačních systémů

Metodika hodnocení informačních systémů se skládá z 6 fází a je rozdělena do 4 dimenzí (Organizace IT oddělení, Přístupová oprávnění, Řízení změn a Provoz IT). Podklady pro provedení fáze dotazníkového šetření, studia dokumentů a interview jsou detailně zpracovány v této příloze. Postup provedení hodnocení je zpracován v kapitole 4.3.

Rozsah hodnocení

V rozsahu hodnocení jsou definovány identifikační otázky a hodnocené systémy. Pro každou otázku je vytvořen unikátní index, který se skládá z označení identifikační otázky P *(Particularize)* a pořadového čísla otázky. Aplikace, operační systém a databáze, které jsou předmětem hodnocení, jsou označeny indexem S *(System)* a pořadovým číslem.

P. Identifikační otázky (otázky P1 – P5)

Index	Otázka	Odpověď	Komentář
P1	Jaká je velikost firmy?	(a) Malý podnik (pod 15 zaměstnanců) (b) Střední podnik (15–250 zaměstnanců) (c) Velký podnik (nad 251 zaměstnanců)	
P2	Jaký je převládající obor podnikání firmy?	(a) Zemědělství (b) Těžba (c) Výrobci (d) Voda, energie, odpady (e) Nemovitosti (f) Obchod (g) Doprava (h) Kultura, sport (i) Telekomunikace, IT, (j) Finance (k) Služby pro podnikatele (l) Ostatní služby	
P3	Kolik let firma realizuje svou činnost?	(a) do 1 roku (b) 2–5 let, (c) 6–10 let (d) více jak 10 let	
P4	Jaké jsou ve firmě vlastnické poměry?	(a) české (b) zahraniční (c) kombinované	
P5	Jaká je velikost IT oddělení?	(a) 0 - outsourcing (b) 1–2 zaměstnanců (c) 3–7 zaměstnanců (d) 7–10 zaměstnanců (e) více jak 10 zaměstnanců	

S. Hodnocené systémy (systémy S1 – Sx)

Index	Aplikace (APP)	Operační systém (OS)	Databáze (DB)	Komentář
S1	S1APP	S1OS	S1DB	

Dotazník

Pro každou otázku ve formě výroku je vytvořen unikátní index, který se skládá z označení dotazníkové otázky Q *(Questionnaire)*, následuje pořadové číslo otázky, zkratka domény (G, A, C nebo O) a odkaz na databázi nedostatků (např. G1). V dotazníku byly použity uzavřené trichotomické otázky (možnost výběru ze tří odpovědí: ano, ne, částečně). Respondent může ke každé otázce přidat krátký komentář.

QG. Organizace IT oddělení (otázky Q1 – Q7)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q1G1	Ve firmě jsou vytvořeny a udržovány formalizované politiky v oblasti IS/ICT.				
Q2G1	Zaměstnanci firmy jsou pravidelně seznamováni s obsahem IS/ICT politik.				
Q3G2	Formalizovaná strategie podniku je vytvořena a aktivně udržována.				
Q4G2	Zaměstnanci firmy jsou pravidelně seznamováni s obsahem strategie podniku.				
Q5G3	Je zavedeno formální řízení rizik zahrnující identifikaci potenciálních hrozeb.				
Q6G4	Ve firmě je jmenován IT manažer, který zodpovídá za správu a vývoj v oblasti IS/ICT.				
Q7G4	IT manažer společnosti není zodpovědný za jiné oblasti podniku (např. logistika, finance, nákup).				

QA. Přístupová oprávnění 1/2 (otázky Q8 – Q9)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q8A1	Ve firmě je zavedený formální proces schvalování nových uživatelských účtů v systému.				
Q9A2	Ve firmě je zavedený formální proces schvalování změn uživatelských oprávnění.				

QA. Přístupová oprávnění 2/2 (otázky Q10 – Q23)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q10A2	Ve firmě jsou vytvořeny a udržovány formalizované politiky v oblasti přístupových oprávnění.				
Q11A2	Zaměstnanci firmy jsou s obsahem politik v oblasti přístupových oprávnění pravidelně seznamováni.				
Q12A3	V případě jakékoli změny pozice zaměstnance jsou modifikovány uživatelská oprávnění v systému.				
Q13A4	IT oddělení je vždy informováno o odchozích zaměstnancích v dostatečném předstihu.				
Q14A5	V případě, že zaměstnanec opouští společnost, uživatelský účet je vždy smazán nebo deaktivován.				
Q15A6	Je zavedena pravidelná kontrola uživatelských účtů.				
Q16A7	Kontrola uživatelských účtů je formalizována a pečlivě vyhodnocována.				
Q17A8	Je zavedena pravidelná kontrola uživatelských oprávnění.				
Q18A8	Kontrola uživatelských oprávnění je formalizována a pečlivě vyhodnocována.				
Q19A9	Je definovaný seznam citlivých transakcí v systému (např. vytvořit účet nebo přiřadit oprávnění).				
Q20A9	Přístup k citlivým transakcím je omezen pouze pro minimální počet pracovníků.				
Q21A9	Seznam pracovníků, kteří mají přístup k citlivým transakcím, je schválen managementem firmy.				
Q22A10	Matice neslučitelných oprávnění je zpracována a pravidelně aktualizována.				
Q23A11	Hesla k uživatelským účtům je nutné měnit v pravidelných intervalech.				

QA. Přístupová oprávnění 2/2 (otázky Q24 – Q30)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q24A11	Hesla k uživatelským účtům musí splňovat podmínku na minimální délku a komplexitu.				
Q25A12	Každý zaměstnanec (včetně IT administrátorů) má své unikátní přihlašovací jméno a heslo.				
Q26A13	Ve firmě neexistuje ani jeden uživatelský účet, který je sdílen mezi zaměstnanci a používán více osobami.				
Q27A13	Administrátorský přístup je vyhrazen pouze minimálnímu počtu pracovníků pouze z IT oddělení.				
Q28A13	Seznam administrátorských účtů je pravidelně kontrolován a schválen managementem firmy.				
Q29A14	Aktivity privilegovaných účtů jsou zaznamenávány a pravidelně kontrolovány.				
Q30A15	Pro vzdálené připojení k systému je implementován software pro šifrování komunikace.				

QC. Řízení změn 1/2 (otázky Q31 – Q37)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q31C1	Ve firmě jsou vytvořeny a udržovány formalizované politiky v oblasti řízení změn.				
Q32C1	Zaměstnanci firmy jsou pravidelně seznamováni s obsahem politiky v oblasti řízení změn.				
Q33C1	Existuje politika pro nasazení mimořádných (emergency) změn.				
Q34C1	Pro každý požadavek na změnu existuje business case (dokument obsahuje přínosy změny a náklady na vývoj).				
Q35C2	Každá změna je před implementací do produkce testována v separátním prostředí.				
Q36C2	Mimořádné (emergency) změny jsou retrospektivně testovány a schváleny po zavedení do produkce.				
Q37C3	Programování, testování a zavádění do produkce je prováděno různými pracovníky (role jsou oddělené).				

QC. Řízení změn 2/2 (otázky Q38 – Q40)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q38C4	Existuje testovací prostředí rozdílné od produkčního zřízené především pro testování změn.				
Q39C5	Interní vývojáři nemají přístup do produkčního prostředí s možností zápisu či aktualizace dat.				
Q40C6	Jakákoli externí entita nemá přístup do produkčního prostředí s možností zápisu či aktualizace dat.				

QO. Provoz IT (otázky Q41 – Q50)

Index	Otázka	Ano	Ne	Částečně	Komentář
Q41O1	Je prováděna a formalizována kontrola přenosu dat mezi aplikacemi.				
Q42O2	Zálohy jsou pravidelně odnášeny mimo firmu na externím médiu pro snížení rizika v případě neočekávané události.				
Q43O2	Kritické systémy, databáze a dokumenty jsou pravidelně zálohovány.				
Q44O3	Zálohy jsou pravidelně kontrolovány a testovány.				
Q45O4	Infrastrukturu používanou ve firmě nelze považovat za zastaralou ve srovnání s trhem či konkurencí.				
Q46O5	Disaster Recovery Plan a Business Contiuity jsou zavedené a pravidelně aktualizované.				
Q47O5	Disaster Recovery Plan a Business Contiuity jsou pravidelně testovány a vyhodnocovány.				
Q48O6	Disaster Recovery Plan a Business Contiuity pokrývající všechna rizika související s hardwarovými a softwarovými výpadky.				
Q49O7	Fyzická bezpečnost serverovny je zajištěná, např. pomocí požárního alarmu, klimatizace, UPS.				
Q50O8	Auditní log citlivých operací je pro produkční prostředí systému zapnutý.				

Studium dokumentů

Pro každou otázku je vytvořen unikátní index, který se skládá z označení dotazníkové otázky D *(Documents)*, následuje pořadové číslo otázky, zkratka domény (G, A, C nebo O) a odkaz na databázi nedostatků (např. G1). Pole s názvem status slouží pro označení dodaných dokumentů a pole komentář pro vložení poznámky v průběhu hodnocení.

Některé dokumenty se vztahují k více nedostatkům: dokument D8A7 má návaznost také na nedostatek A8, D15C2 se vztahuje i k C3 a D20O5 je provázaný s nedostatkem O6.

DG. Organizace IT oddělení (dokumenty D1 – D4)

Index	Dokument	Status	Komentář
D1G1	Obecná politika v oblasti IS/ICT. IT strategie společnosti.		
D2G2	Obchodní strategie společnosti.		
D3G3	Výstup hodnocení rizik. Výsledek interního/externího auditu.		
D4G4	Organizační struktura firmy a IT oddělení. Rozdělení rolí v IT oddělení.		

DA. Přístupová oprávnění 1/2 (dokumenty D5 – D9)

Index	Dokument	Status	Komentář
D5A1-2	Politika pro přístupová oprávnění (zakládání a deaktivace účtů, přidělování oprávnění).		
D6A3-5	Seznam aktivních uživatelů v systému včetně data posledního přihlášení.		
D7A3-5	Seznam příchozích a odchozích zaměstnanců ve sledovaném období.		
D8A6-8	Výstupy z periodické kontroly uživatelských účtů a oprávnění.		
D9A9	Seznam pracovníků, kteří mají přístup k citlivým transakcím.		

DA. Přístupová oprávnění 2/2 (dokumenty D10 – D13)

Index	Dokument	Status	Komentář
D10A10	Matice neslučitelných oprávnění.		
D11A11	Politika hesel nastavená v systému.		
D12 A12-13	Seznam administrátorských účtů v systému.		
D13A14	Záznam o provedení kontroly aktivit privilegovaných účtů.		

DC. Řízení změn (dokumenty D14 – D16)

Index	Dokument	Status	Komentář
D14C1	Politika pro řízení změn. Politika pro nasazení mimořádných změn.		
D15C2-3	Seznam provedených změn v produkčním prostředí obsahující popis změny a záznamu o programování, testování a nasazení.		
D16C4	Přehled vývojových, testovacích a produkčních prostředí.		

DO. Provoz IT (dokumenty D17 – D20)

Index	Dokument	Status	Komentář
D17O1	Přehled rozhraní mezi aplikacemi. Záznam o testování přenosu dat.		
D18O2-3	Konfigurace plánu zálohování. Záznam o provedení pravidelné kontroly záloh.		
D19O4	Přehled IT a síťové infrastruktury.		
D20O5-6	Disaster Recovery Plan (DRP) a Business Continuity Plan (BCP). Výsledek testování obou plánů.		

Interview

Pro každé téma je vytvořen unikátní index, který se skládá z označení téma rozhovoru I *(Interview)*, následuje pořadové číslo tématu, zkratka domény (G, A, C nebo O) a odkaz na databázi nedostatků (např. G1). Témata jsou sloučena podle segmentu. Jedno téma tedy může vést na více nedostatků a tomu odpovídá i index (např. I2G2-4 má návaznost na nedostatky G2, G3 a G4). Pole s názvem status slouží pro označení provedených interview a pole komentář pro vložení poznámky v průběhu hodnocení.

IG. Organizace IT oddělení (téma I1 – I4)

Index	Téma	Status	Komentář
I1G1	Politiky a směrnice v oblasti IS/ICT (zahrnuté oblasti ve směrnicích a jejich dostupnost, hlavní systémy, aplikace a databáze, pokrytí procesů).		
I2G2-G4	Řízení IT oddělení (strategie podniku a její návaznost na IS/ICT, soulad se zákony a normami, realizace a vyhodnocení analýzy rizik, dopad na IS/ICT, metodika a frekvence hodnocení, organizace IT oddělení, rozdělení rolí, pravomocí a odpovědností v IT oddělení).		

IA. Přístupová oprávnění 1/2 (téma I3 – I5)

Index	Téma	Status	Komentář
I3A1-5	Přidávání a odebírání uživatelských oprávnění (popis procesu schvalování uživatelských účtů a oprávnění, systémy pro evidenci požadavků, využití SOO a AD, modifikace oprávnění v případě přechodu zaměstnance na jinou pozici, proces odebrání práv odchozím zaměstnancům, časová posloupnost procesu).		
I4A6-8	Pravidelná kontrola uživatelských oprávnění (popis procesu kontroly, frekvence a vyhodnocení, zodpovědnost za kontrolu).		
I5A9-10	Rozdělení pravomocí (definování citlivých transakcí, monitorování přístupu k citlivým transakcím, matice neslučitelných oprávnění).		

IA. Přístupová oprávnění 2/2 (téma I6 – I8)

Index	Téma	Status	Komentář
I6A11	Heslová politika (politiky a procedury, které se používají pro konfiguraci hesel, správa hesel na uživatelské i administrátorské úrovni, sdílené účty a hesla, délka, komplexnost, expirace hesel, další bezpečností parametry).		
I7A12-14	Administrátorské účty (administrátorské účty pro aplikace, systémy a databáze, proces přidělování, odebírání a modifikace oprávnění, logování aktivit administrátorů, sdílené účty, zaměstnanci s administrátorským účtem).		
I8A15	Vzdálený přístup (proces přidělování, odebírání a modifikace oprávnění pro vzdálený přístup, zabezpečení vzdáleného přístupu).		

IC. Řízení změn (téma I9 – I10)

Index	Téma	Status	Komentář
I9C1-4	Proces změnového řízení (řízení aktivit a proces změnového řízení a vývoje aplikací ve společnosti, testování a ověřování kvality, implementace do produkčního prostředí, používaná vývojová a testovací prostředí, rozdělení pravomocí, kategorizace změn, mimořádné emergency změny, systémy pro evidenci požadavků).		
I10C5-6	Přístup do produkčního prostředí (zapojení dodavatelů a interních vývojářů, rozdělení pravomocí v rámci implementace do produkčního prostředí, SLA).		

IO. Provoz IT 1/2 (téma I11)

Index	Téma	Status	Komentář
I11O1	Rozhraní mezi aplikacemi (architektura systémů a rozhraní mezi nimi, zpracování dat, monitorování přenosu dat, frekvence kontroly, řešení chyb).		

IO. Provoz IT 2/2 (téma I12 – I15)

Index	Téma	Status	Komentář
I12O2-3	Zálohování (proces zálohování, zálohovaná data, frekvence zálohování dat, proces změny konfigurace zálohování, monitorování a řešení chyb, lokace zálohových médií, pravidelné testování obnovitelnosti záloh).		
I13O4-6	Plány obnovy v případě provozních problémů (Disaster Recovery Plan, Business Continuity, aktualizace a dostupnost plánů, analýza rizik s posouzením dopadu, opatření v případě havárie, role a rozdělení odpovědností, definice kroků při obnově systému, analýza klíčových procesů, záložní plán v případě výpadku kritických aplikací, používaná zařízení, mobilní komunikace, operační systémy, připojení k internetu).		
I14O7	Fyzická bezpečnost (bezpečnostní perimetr, chráněna před selháním napájení, požární ochrana).		
I15O8	Logování (záznam aktivit uživatelů na úrovni operačního systému, databáze a aplikace, definování kritických oblastí, proces kontroly).		

Příloha 5 – Výsledky případových studií

Výsledky případové studie v oblasti malých firem (část 1/2)

Index	Nedostatek	Dotazník	Studium dokumentů	Interview	Vyhodnocení
G1	IT politiky nejsou formálně dokumentovány, schváleny a publikovány.	Q1-2	D1	I1	Nedostatek 1
G2	Podnik nemá ucelenou strategii vedení a správy společnosti.	Q3-4	D2	I2	Bez nálezu
G3	Nedostatečné řízení rizik v oblasti IS/ICT.	Q5	D3	I2	Nedostatek 2
G4	IT oddělení není řízeno centrálně a nezodpovídá za některé IT oblasti.	Q6-7	D4	I2	Bez nálezu
A1	V produkčním systému je aktivní a užívaný účet, který není schválený.	Q8	D5	I3	Bez nálezu
A2	Proces udělování a odebírání přístupových oprávnění není řádně nastaven.	Q9-11	D5	I3	Nedostatek 3
A3	Žádosti o přidělení přístupových oprávnění nejsou řádně zdokumentovány.	Q12-13	D6-7	I3	Bez nálezu
A4	V produkčním systému je aktivní a užívaný účet zaměstnance, který již ve společnosti nepracuje.	Q13	D6-7	I3	Bez nálezu
A5	Uživatelské účty nejsou odebrány včas.	Q14	D6-7	I3	Nedostatek 4
A6	Není prováděna periodická kontrola přístupových oprávnění.	Q15	D8	I4	Nedostatek 5
A7	Periodická kontrola přístupových oprávnění není formalizovaná.	Q16	D8	I4	Nedostatek 5 (viz A6)
A8	Periodická kontrola přístupových oprávnění není dostatečná.	Q17-18	D8	I4	Nedostatek 5 (viz A6)
A9	Uživatelé mají přístup k citlivým transakcím.	Q19-21	D9	I5	Bez nálezu
A10	Není zpracována matice neslučitelných oprávnění.	Q22	D10	I5	Nedostatek 6
A11	Nedostatečné nastavení heslové politiky.	Q23-24	D11	I6	Bez nálezu
A12	Sdílený administrátorský účet.	Q25	D12	I7	Bez nálezu

Výsledky případové studie v oblasti malých firem (část 2/2)

Index	Nedostatek	Dotazník	Studium dokumentů	Interview	Vyhodnocení
A13	Uživatelé s neomezeným oprávněním.	Q26-28	D12	I7	Bez nálezu.
A14	Nedostatečné monitorování aktivit privilegovaných účtů.	Q29	D13	I7	Nedostatek 7
A15	Vzdálený přístup do produkčního systému není monitorován.	Q30	-	I8	Bez nálezu
C1	Proces změnového řízení není řádně nastaven.	Q31-34	D14	I9	Nehodnoceno.
C2	Změna není testovaná před implementací do produkčního prostředí.	Q35-36	D15	I9	Nehodnoceno.
C3	Nedostatečné rozdělení pravomocí v oblasti změnového řízení.	Q37	D15	I9	Nehodnoceno.
C4	Testovací prostředí není vytvořeno, změny jsou implementovány přímo do produkce.	Q38	D16	I9	Nehodnoceno.
C5	Neomezený přístup interních vývojářů do produkčního prostředí.	Q39	-	I10	Nehodnoceno.
C6	Neomezený přístup dodavatele do produkčního prostředí.	Q40	-	I10	Nehodnoceno.
O1	Nedostatečné monitorování rozhraní mezi aplikacemi.	Q41	D17	I11	Nehodnoceno.
O2	Proces zálohování dat je nedostatečný.	Q42-43	D18	I12	Bez nálezu
O3	Nedostatečné testování záloh.	Q44	D18	I12	Bez nálezu
O4	Zastaralá infrastruktura.	Q45	D19	I13	Bez nálezu
O5	Není implementován havarijní plán a plán kontinuity obchodních činností	Q46-47	D20	I13	Nedostatek 8
O6	Havarijní plán a plán kontinuity nepokrývají všechna rizika.	Q48	D20	I13	Nedostatek 8 (viz O5)
O7	Fyzická bezpečnost serverovny.	Q49	-	I14	Bez nálezu
O8	Vypnuté logování produkční databáze.	Q50	-	I15	Bez nálezu

Výsledky případové studie v oblasti středních firem (část 1/2)

Index	Nedostatek	Dotazník	Studium dokumentů	Interview	Vyhodnocení
G1	IT politiky nejsou formálně dokumentovány, schváleny a publikovány.	Q1-2	D1	I1	Bez nálezu
G2	Podnik nemá ucelenou strategii vedení a správy společnosti.	Q3-4	D2	I2	Bez nálezu
G3	Nedostatečné řízení rizik v oblasti IS/ICT.	Q5	D3	I2	Bez nálezu
G4	IT oddělení není řízeno centrálně a nezodpovídá za některé IT oblasti.	Q6-7	D4	I2	Bez nálezu
A1	V produkčním systému je aktivní a užívaný účet, který není schválený.	Q8	D5	I3	Nedostatek 1
A2	Proces udělování a odebírání přístupových oprávnění není řádně nastaven.	Q9-11	D5	I3	Bez nálezu
A3	Žádosti o přidělení přístupových oprávnění nejsou řádně zdokumentovány.	Q12-13	D6-7	I3	Bez nálezu
A4	V produkčním systému je aktivní a užívaný účet zaměstnance, který již ve společnosti nepracuje.	Q13	D6-7	I3	Bez nálezu
A5	Uživatelské účty nejsou odebrány včas.	Q14	D6-7	I3	Bez nálezu
A6	Není prováděna periodická kontrola přístupových oprávnění.	Q15	D8	I4	Bez nálezu
A7	Periodická kontrola přístupových oprávnění není formalizovaná.	Q16	D8	I4	Bez nálezu
A8	Periodická kontrola přístupových oprávnění není dostatečná.	Q17-18	D8	I4	Nedostatek 2
A9	Uživatelé mají přístup k citlivým transakcím.	Q19-21	D9	I5	Bez nálezu
A10	Není zpracována matice neslučitelných oprávnění.	Q22	D10	I5	Bez nálezu
A11	Nedostatečné nastavení heslové politiky.	Q23-24	D11	I6	Bez nálezu
A12	Sdílený administrátorský účet.	Q25	D12	I7	Bez nálezu

Výsledky případové studie v oblasti středních firem (část 2/2)

Index	Nedostatek	Dotazník	Studium dokumentů	Interview	Vyhodnocení
A13	Uživatelé s neomezeným oprávněním.	Q26-28	D12	I7	Bez nálezu
A14	Nedostatečné monitorování aktivit privilegovaných účtů.	Q29	D13	I7	Bez nálezu
A15	Vzdálený přístup do produkčního systému není monitorován.	Q30	-	I8	Bez nálezu
C1	Proces změnového řízení není řádně nastaven.	Q31-34	D14	I9	Bez nálezu
C2	Změna není testovaná před implementací do produkčního prostředí.	Q35-36	D15	I9	Nedostatek 3
C3	Nedostatečné rozdělení pravomocí v oblasti změnového řízení.	Q37	D15	I9	Bez nálezu
C4	Testovací prostředí není vytvořeno, změny jsou implementovány přímo do produkce.	Q38	D16	I9	Bez nálezu
C5	Neomezený přístup interních vývojářů do produkčního prostředí.	Q39	-	I10	Nedostatek 4
C6	Neomezený přístup dodavatele do produkčního prostředí.	Q40	-	I10	Bez nálezu
O1	Nedostatečné monitorování rozhraní mezi aplikacemi.	Q41	D17	I11	Bez nálezu
O2	Proces zálohování dat je nedostatečný.	Q42-43	D18	I12	Bez nálezu
O3	Nedostatečné testování záloh.	Q44	D18	I12	Bez nálezu
O4	Zastaralá infrastruktura.	Q45	D19	I13	Bez nálezu
O5	Není implementován havarijní plán a plán kontinuity obchodních činností	Q46-47	D20	I13	Nedostatek 5
O6	Havarijní plán a plán kontinuity nepokrývají všechna rizika.	Q48	D20	I13	Bez nálezu
O7	Fyzická bezpečnost serverovny.	Q49	-	I14	Bez nálezu
O8	Vypnuté logování produkční databáze.	Q50	-	I15	Bez nálezu

Výsledky případové studie v oblasti velkých firem (část 1/2)

Index	Nedostatek	Dotazník	Studium dokumentů	Interview	Vyhodnocení
G1	IT politiky nejsou formálně dokumentovány, schváleny a publikovány.	Q1-2	D1	I1	Bez nálezu
G2	Podnik nemá ucelenou strategii vedení a správy společnosti.	Q3-4	D2	I2	Bez nálezu
G3	Nedostatečné řízení rizik v oblasti IS/ICT.	Q5	D3	I2	Bez nálezu
G4	IT oddělení není řízeno centrálně a nezodpovídá za některé IT oblasti.	Q6-7	D4	I2	Bez nálezu
A1	V produkčním systému je aktivní a užívaný účet, který není schválený.	Q8	D5	I3	Bez nálezu
A2	Proces udělování a odebírání přístupových oprávnění není řádně nastaven.	Q9-11	D5	I3	Bez nálezu
A3	Žádosti o přidělení přístupových oprávnění nejsou řádně zdokumentovány.	Q12-13	D6-7	I3	Bez nálezu
A4	V produkčním systému je aktivní a užívaný účet zaměstnance, který již ve společnosti nepracuje.	Q13	D6-7	I3	Bez nálezu
A5	Uživatelské účty nejsou odebrány včas.	Q14	D6-7	I3	Nedostatek 1
A6	Není prováděna periodická kontrola přístupových oprávnění.	Q15	D8	I4	Bez nálezu
A7	Periodická kontrola přístupových oprávnění není formalizovaná.	Q16	D8	I4	Bez nálezu
A8	Periodická kontrola přístupových oprávnění není dostatečná.	Q17-18	D8	I4	Bez nálezu
A9	Uživatelé mají přístup k citlivým transakcím.	Q19-21	D9	I5	Bez nálezu
A10	Není zpracována matice neslučitelných oprávnění.	Q22	D10	I5	Nedostatek 2
A11	Nedostatečné nastavení heslové politiky.	Q23-24	D11	I6	Bez nálezu
A12	Sdílený administrátorský účet.	Q25	D12	I7	Bez nálezu

Výsledky případové studie v oblasti velkých firem (část 2/2)

Index	Nedostatek	Dotazník	Studium dokumentů	Interview	Vyhodnocení
A13	Uživatelé s neomezeným oprávněním.	Q26-28	D12	I7	Bez nálezu
A14	Nedostatečné monitorování aktivit privilegovaných účtů.	Q29	D13	I7	Bez nálezu
A15	Vzdálený přístup do produkčního systému není monitorován.	Q30	-	I8	Bez nálezu
C1	Proces změnového řízení není řádně nastaven.	Q31-34	D14	I9	Bez nálezu
C2	Změna není testovaná před implementací do produkčního prostředí.	Q35-36	D15	I9	Bez nálezu
C3	Nedostatečné rozdělení pravomocí v oblasti změnového řízení.	Q37	D15	I9	Nedostatek 3
C4	Testovací prostředí není vytvořeno, změny jsou implementovány přímo do produkce.	Q38	D16	I9	Bez nálezu
C5	Neomezený přístup interních vývojářů do produkčního prostředí.	Q39	-	I10	Bez nálezu
C6	Neomezený přístup dodavatele do produkčního prostředí.	Q40	-	I10	Bez nálezu
O1	Nedostatečné monitorování rozhraní mezi aplikacemi.	Q41	D17	I11	Bez nálezu
O2	Proces zálohování dat je nedostatečný.	Q42-43	D18	I12	Bez nálezu
O3	Nedostatečné testování záloh.	Q44	D18	I12	Nedostatek 4
O4	Zastaralá infrastruktura.	Q45	D19	I13	Bez nálezu
O5	Není implementován havarijní plán a plán kontinuity obchodních činností	Q46-47	D20	I13	Bez nálezu
O6	Havarijní plán a plán kontinuity nepokrývají všechna rizika.	Q48	D20	I13	Bez nálezu
O7	Fyzická bezpečnost serverovny.	Q49	-	I14	Bez nálezu
O8	Vypnuté logování produkční databáze.	Q50	-	I15	Bez nálezu

Příloha 6 – Curriculum Vitae

Jméno:	**Ing. Lukáš Novák**
Datum narození:	18. 2. 1988
Adresa:	Zdráhalova 49, 613 00 Brno
E-mail:	novakl@fbm.vutbr.cz

Vzdělání

Vysoké učení technické v Brně, Fakulta podnikatelská (2012 – současnost)
Doktorský studijní obor Řízení a ekonomika podniku

Vysoké učení technické v Brně, Fakulta podnikatelská (2010–2012)
Magisterský studijní obor Informační management / s vyznamenáním

Vysoké učení technické v Brně, Fakulta podnikatelská (2007–2010)
Bakalářský studijní obor Manažerská informatika / s vyznamenáním

Gymnázium Elgartova, Brno (2003–2007)
Maturita z českého jazyka, matematiky, němčiny a informatiky / s vyznamenáním

Ocenění

Cena děkanky FP VUT v Brně za vynikající studijní výsledky (2012)
Cena rektora VUT v Brně za mimořádně přínosnou diplomovou práci (2012)

Zahraniční stáže

PricewaterhouseCoopers LLP / Philadelphia (10/2015, 10/2017)
Technische Universität Wien / Fakultät für Bauingenieurwesen (09/2013)
Nottingham Trent University / Nottingham Business School (11-12/2012)

Praxe

PricewaterhouseCoopers Audit s.r.o. (2014 – současnost)
Risk Assurance, System and Process Audit, Data Confidence

Vysoké učení technické v Brně, Fakulta podnikatelská (2012 - současnost)
Ústav informatiky: výuka předmětů Datové a funkční modelování, Management informačních systémů a Informatika pro ekonomy
Ústav managementu: vědecký pracovník
Útvar koordinace projektů.
Člen organizačního výboru mezinárodních konferencí
Spolupráce Fakulty podnikatelské VUT v Brně a PricewaterhouseCoopers Audit s.r.o. v oblasti zadávání a vedení bakalářských a diplomových prací

Živnostenské oprávnění (2011–2014)
Poradenství v oblasti IS/ICT, vývoj a správa internetových stránek

Další vzdělání

Anglický jazyk
First Certificate in English, University of Cambridge, level B2 (2011)

Německý jazyk
Actilingua Academy, Austria, Grundstufe 2 (2005) a Grundstufe 3 (2006)

Management informační bezpečnosti
Specialista dle norem řady ISO 27000 (2013)

Řešené projekty

Collaboration in Higher Education for Digital Transformation in European Business CHEDTEB
Mezinárodní program Erasmus+ program
Zahájení: 1. 9. 2017, ukončení: 31. 8. 2019

MOST – Moderní a otevřené studium techniky
Projekty ESF, OP VVV PO2 ESF výzva pro vysoké školy
Zahájení: 1. 9. 2017, ukončení: 31. 12. 2022

Podnikání v éře Průmyslu 4.0
Projekt specifického výzkumu, VUT v Brně, číslo FP-S-17-4634
Zahájení: 1. 1. 2017, ukončení: 31. 12. 2018

Efektivní využití ICT a kvantitativních metod pro optimalizaci podnikových procesů
Projekt specifického výzkumu, VUT v Brně, číslo FP-S-15-2787
Zahájení: 1. 1. 2015, ukončení: 31. 12. 2016

Využití ICT a matematických metod při řízení podniku
Projekt specifického výzkumu, VUT v Brně, číslo FP-S-13-2148
Zahájení: 1. 1. 2013, ukončení: 31. 12. 2014

Příloha 7 – Publikační činnost

Články v recenzovaném sborníku z konference zahrnutém do databází SCOPUS a Thomson Reuters

NOVÁK, Lukáš, 2013. The relationship of the GDP and ICT Spending and Investment: Analysis of data between 2006 and 2011 in the Czech Republic. *Vision 2020: Innovation, Development Sustainability, and Economic Growth Proceedings.* Vienna: IBIMA.

NOVÁK, Lukáš, 2014a. Analysis of the Effect of Economic Development on Expenditures and Investments into IT in the Czech Republic, Poland, Slovakia and Hungary. *Vision 2020: Sustainable Growth, Economic Development, and Global Competitiveness*. Valencia: IBIMA.

NOVÁK, Lukáš, 2014b. The Success Factors in an International Company: A Case Study. *Crafting Global Competitive Economies: 2020 Vision Strategic Planning & Smart Implementation*. Milano: IBIMA.

NOVÁK, Lukáš, 2015a. Development of an Information Strategy and Proposed Changes in Corporate Informatics on the Basis of an Application of Methods of Scientific Analysis to the Information System Evaluation: Case Study. *Innovation Vision 2020: From Regional Development Sustainability to Global Economic Growth.* Amsterdam: IBIMA.

NOVÁK, Lukáš, 2015b. Analysis of Methods for the Evaluation of Information Systems: Critical Comparison by Selected Criteria. Madrid: IBIMA.

Články v recenzovaném sborníku z konference

NOVÁK, Lukáš, 2012. *Metody hodnocení efektivnosti informačních systémů: základní analýza a srovnání vytvořených metod*. *Mezinárodní workshop doktorandských prací*. Vysoké učení technické v Brně. Fakulta podnikatelská.

NOVÁK, Lukáš, 2016. Evaluation of Information Systems in Medium – sized and Large Businesses. *International Scientific Conference Economics and Management.* Brno: Brno University of Technology.